SUSE Linux Referência

www.novell.com

10.0 | 09/13/2005

Referência

List of Authors: Jörg Arndt, Stefan Behlert, Frank Bodammer, James Branam, Volker Buzek, Klara Cihlarova, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Thorsten Dubiel, Torsten Duwe, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Joachim Gleißner, Carsten Groß, Andreas Grünbacher, Berthold Gunreben, Franz Hassels, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Edith Parzefall, Peter Pöml, Thomas Renninger, Hannes Reinecke, Thomas Rölz, Heiko Rommel, Marcus Schäfer, Thomas Schraitle, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz

A propriedade intelectual desta publicação é da Novell Inc.

O seu conteúdo pode ser duplicado, em parte ou integralmente, desde que um rótulo de copyright esteja visivelmente localizado em cada cópia.

Todas as informações deste manual foram compiladas com a maior atenção possível aos detalhes. Entretanto, isso não garante uma precisão absoluta. O SUSE LINUX GmbH, os autores ou os tradutores não deverão ser responsabilizados por possíveis erros ou conseqüências decorrentes.

Muitas das descrições de software e hardware mencionadas neste manual são marcas registradas. Todos os nomes comerciais estão sujeitos a restrições de copyright e podem ser marcas registradas. O SUSE LINUX GmbH está essencialmente em conformidade com a ortografia do fabricante. Os nomes de produtos e as marcas registradas que aparecem neste manual (com ou sem notação específica) estão igualmente sujeitos às leis de proteção de marcas registradas e comerciais e, portanto, enquadram-se em restrições de copyright.

Envie sugestões e comentários para documentation@suse.de.

Contents

Sobre este guia **xv**

Parte I Cenários de distribuição avançados **19**

1 Instalação remota **21**

1.1 Cenários de instalação para instalação remota 21
1.2 Configurando o servidor que mantém as fontes de instalação 30
1.3 Preparando a inicialização do sistema de destino 40
1.4 Inicializando o sistema de destino para instalação 50
1.5 Monitorando o processo de instalação 55

2 Configuração de disco avançada **59**

2.1 Nomes permanentes para dispositivos SCSI 59
2.2 Configuração da LVM 60
2.3 Configuração de RAID de software 67

Parte II Internet **73**

3 Browser da Web Konqueror **75**

3.1 Navegação em guias 76
3.2 Gravando páginas da Web e elementos gráficos 77
3.3 Palavras-chave da Internet 77
3.4 Favoritos 78
3.5 Java e JavaScript 79
3.6 Para obter mais informações 79

4 Firefox **81**

4.1 Navegando em sites na Web 81
4.2 Localizando informações 83
4.3 Gerenciando marcadores 83
4.4 Usando o gerenciador de downloads 86
4.5 Personalizando o Firefox 86
4.6 Imprimindo no Firefox 89
4.7 Mais informações 90

5 Linphone—VoIP para o Linux Desktop **91**

5.1 Configuração do Linphone 91
5.2 Teste do Linphone 97
5.3 Realização de chamada 97
5.4 Para atender uma chamada 99
5.5 O Bloco de Endereços 99
5.6 Solução de problemas 100
5.7 Glossário 101
5.8 Mais informações 102

6 Criptografia com KGpg **103**

6.1 Gerando um novo par de chaves 103
6.2 Exportando a chave pública 105
6.3 Importando chaves 106
6.4 Caixa de diálogo do servidor de chaves 107
6.5 Criptografia de texto e arquivo 110
6.6 Para obter mais informações 111

Parte III Multimídia **113**

7 Som no Linux **115**

7.1 Mixers 115
7.2 Leitores multimídia 120
7.3 CDs: Reprodução e ripagem 125
7.4 Gravação no disco rígido com o Audacity 130
7.5 Gravação direta e reprodução de arquivos WAV 134

8 TV, vídeo, rádio e webcam **135**

8.1 Assistindo TV com o motv 135
8.2 Suporte ao texto de vídeo 138
8.3 Webcams e motv 138

8.4 nxtvepg – Revista de TV para seu PC 139
8.5 Assistindo transmissões de vídeo digital com o xawtv4 141

9 K3b — Gravando CDs ou DVDs 145

9.1 Criando um CD de dados 145
9.2 Criando um CD de áudio 149
9.3 Copiando um CD ou DVD 150
9.4 Gravando imagens ISO 151
9.5 Criando um CD ou DVD multissessão 151
9.6 Mais informações 152

Parte IV Office 153

10 Suíte para escritórios OpenOffice.org 155

10.1 Compatibilidade com outros aplicativos do Office 156
10.2 Processamento de texto com o Writer 157
10.3 Apresentando o Calc 160
10.4 Apresentando o Impress 161
10.5 Apresentando o Base 161
10.6 Mais informações 162

11 Evolution: programa de e-mail e calendário 165

11.1 Importando e-mails de outros programas de e-mail 165
11.2 Visão geral sobre o Evolution 166
11.3 Correio 167
11.4 Contatos 172
11.5 Calendários 174
11.6 Sincronizando dados com dispositivos portáteis 176
11.7 Evolution para usuários do GroupWise 176
11.8 Para obter mais informações 177

12 Kontact: um programa de e-mail e calendário 179

12.1 Importando e-mail de outros programas de mensagens 179
12.2 Visão geral do Kontact 180
12.3 Correio 182
12.4 Contatos 187
12.5 Calendário 190
12.6 Sincronizando dados com um dispositivo portátil 192
12.7 Kontact para usuários do GroupWise 192
12.8 Mais informações 194

13 Sincronizando um computador portátil com o KPilot **195**

13.1 Conduítes usados pelo KPilot 196
13.2 Configurando a conexão do dispositivo portátil 197
13.3 Configurando o conduíte do KAddressBook 198
13.4 Gerenciando itens de afazeres e eventos 199
13.5 Trabalhando com o KPilot 200

14 Usando o Beagle **203**

14.1 Indexando dados 204
14.2 Pesquisando dados 206

Parte V Gráficos **209**

15 Câmeras digitais e Linux **211**

15.1 Conectando a câmera 211
15.2 Acessando a câmera 212
15.3 Usando o Konqueror 213
15.4 Usando o Digikam 213
15.5 Usando o f-spot 223
15.6 Mais informações 231

16 Kooka — Aplicativo de digitalização **233**

16.1 Visualização 234
16.2 Digitalização final 235
16.3 Menus 236
16.4 Galeria 237
16.5 Reconhecimento Óptico de Caracteres 238

17 Manipulando gráficos com o GIMP **241**

17.1 Formatos gráficos 241
17.2 Iniciando o GIMP 242
17.3 Noções básicas do GIMP 244
17.4 Gravando imagens 245
17.5 Imprimindo imagens 247
17.6 Para obter mais informações 248

Parte VI Mobilidade **251**

18 Computação móvel com o Linux **253**

18.1 Laptops 253
18.2 Hardware móvel 260
18.3 Telefones celulares e PDAs 261
18.4 Mais informações 262

19 PCMCIA **263**

19.1 Hardware 263
19.2 Software 264

20 System Configuration Profile Management **265**

20.1 Terminologia 266
20.2 Usando o Gerenciador de Perfis do YaST 266
20.3 Configurando o SCPM com a linha de comando 270
20.4 Usando o applet Seletor de Perfil 274
20.5 Solução de problemas 274
20.6 Selecionando um perfil ao inicializar o sistema 275
20.7 Mais informações 275

21 Gerenciamento de energia **277**

21.1 Funções de economia de energia 278
21.2 APM 279
21.3 ACPI 280
21.4 Descanso do disco rígido 287
21.5 O Pacote powersave 289
21.6 O módulo Gerenciamento de energia YaST 297

22 Comunicação sem fio **303**

22.1 LAN sem fio 303
22.2 Bluetooth 314
22.3 Transmissão de dados infravermelhos 325

Parte VII Administração **329**

23 Segurança no Linux **331**

23.1 Mascaramento e firewalls 331

23.2 SSH: operações seguras de rede 342
23.3 Criptografando partições e arquivos 348
23.4 Segurança e confidencialidade 351

24 Listas de controle de acesso no Linux 365

24.1 Vantagens das ACLs 365
24.2 Definições 366
24.3 Gerenciando ACLs 367
24.4 Suporte a ACL em aplicativos 375
24.5 Para obter mais informações 376

25 Utilitários de monitoramento do sistema 377

25.1 Lista de arquivos abertos: `lsof` 378
25.2 Arquivos de acesso do usuário: `fuser` 379
25.3 Propriedades de arquivo: `stat` 379
25.4 Dispositivos USB: `lsusb` 380
25.5 Informações sobre um dispositivo SCSI: `scsiinfo` 381
25.6 Processos: `top` 381
25.7 Lista de processos: `ps` 382
25.8 Árvore de processos: `pstree` 384
25.9 Quem está fazendo o quê: `w` 384
25.10 Uso da memória: `free` 385
25.11 Buffer do anel de kernel: `dmesg` 386
25.12 Sistemas de arquivos e sua utilização: `mount`, `df` e `du` 386
25.13 O sistema de arquivos `/proc` 387
25.14 `vmstat`, `iostat` e `mpstat` 389
25.15 `procinfo` 390
25.16 Recursos PCI: `lspci` 391
25.17 Chamadas do sistema de uma execução de programa: `strace` 392
25.18 Chamadas da biblioteca de uma execução de programa: `ltrace` 393
25.19 Especificação da biblioteca necessária: `ldd` 393
25.20 Informações adicionais sobre binários ELF 394
25.21 Comunicação entre processos: `ipcs` 395
25.22 Medição do tempo com `time` 395

Parte VIII Sistema 397

26 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits 399

26.1 Suporte ao tempo de execução 399
26.2 Desenvolvimento de software 400

26.3 Compilação de software em plataformas biarch 401
26.4 Especificações do kernel 402

27 Trabalhando com o Shell 403

27.1 Usando Bash na linha de comando 403
27.2 Usuários e permissões de acesso 414
27.3 Comandos importantes do Linux 420
27.4 Editor vi 432

28 Inicializando e configurando um sistema Linux 437

28.1 Processo de inicialização do Linux 437
28.2 O processo init 441
28.3 Configuração do sistema via /etc/sysconfig 450

29 O Carregador de Boot 453

29.1 Gerenciamento de boot 454
29.2 Selecionando um carregador de boot 455
29.3 Inicializando com o GRUB 455
29.4 Configurando o carregador de boot com o YaST 466
29.5 Desinstalando a controladora de boot do Linux 471
29.6 Criando CDs de boot 472
29.7 A tela gráfica do SUSE 473
29.8 Solução de problemas 473
29.9 Mais informações 475

30 Recursos especiais do SUSE Linux 477

30.1 Informações sobre pacotes de software especiais 477
30.2 Consoles virtuais 484
30.3 Mapeamento de teclado 485
30.4 Configurações de idioma e específicas de país 486

31 Operação da impressora 491

31.1 Fluxo de trabalho do sistema de impressão 493
31.2 Métodos e protocolos de conexão de impressoras 493
31.3 Instalação do software 494
31.4 Configuração da impressora 495
31.5 Configuração de aplicativos 501
31.6 Recursos especiais do SUSE Linux 502
31.7 Solução de problemas 507

32 O sistema hotplug **517**

32.1 Dispositivos e interfaces 518
32.2 Eventos hotplug 519
32.3 Configuração do dispositivo hotplug 519
32.4 Carregamento de módulo automático 522
32.5 O Script de boot coldplug 522
32.6 Análise de erro 522

33 Nós de dispositivo dinâmicos com udev **525**

33.1 Criando regras 526
33.2 Substituição de marcador 527
33.3 Correspondência de padrões em chaves 527
33.4 Seleção de chaves 527
33.5 Nomes persistentes para dispositivos de armazenamento em massa . . . 529

34 Sistemas de arquivos no Linux **531**

34.1 Terminologia 531
34.2 Principais sistemas de arquivos no Linux 532
34.3 Outros sistemas de arquivos suportados 539
34.4 LFS (Large File Support - Suporte a Arquivos Grandes) no Linux 541
34.5 Para obter mais informações 542

35 O sistema X Window **545**

35.1 Configuração do X11 com o SaX2 545
35.2 Otimizando a configuração do X 547
35.3 Instalando e configurando fontes 553
35.4 Configuração 3D do OpenGL 559

36 Autenticação com o PAM **563**

36.1 Estrutura de um arquivo de configuração PAM 564
36.2 A configuração PAM do sshd 566
36.3 Configuração de módulos PAM 568
36.4 Mais informações 570

37 Virtualização com o Xen **573**

37.1 Instalação do Xen 575
37.2 Instalação do domínio 576
37.3 Configurando um domínio convidado do Xen 579
37.4 Iniciando e controlando domínios do Xen 581

37.5 Para obter mais informações 582

Parte IX Serviços 583

38 Rede básica 585

38.1 Roteamento e endereços IP 588
38.2 IPv6— A Internet da próxima geração 591
38.3 Resolução de nomes 601
38.4 Configurando uma conexão de rede com o YaST 602
38.5 Configurando uma conexão de rede manualmente 613
38.6 smpppd como Assistente de Discagem 625

39 Serviços SLP na rede 629

39.1 Registrando seus próprios serviços 629
39.2 Front ends de SLP no SUSE Linux 630
39.3 Ativando o SLP 631
39.4 Mais informações 631

40 Domain Name System (Sistema de Nomes de Domínio) 633

40.1 Informações básicas sobre o DNS 633
40.2 Configuração com o YaST 633
40.3 Iniciando o BIND do servidor de nomes 641
40.4 O arquivo de configuração /etc/named.conf 643
40.5 Arquivos de zona 648
40.6 Atualização dinâmica dos dados da zona 652
40.7 Transações de segurança 652
40.8 Segurança do DNS 653
40.9 Para obter mais informações 654

41 Usando o NIS 655

41.1 Configurando servidores NIS usando o YaST 655
41.2 Configurando clientes NIS 660

42 Compartilhando sistemas de arquivos com o NFS 663

42.1 Importando sistemas de arquivos com o YaST 663
42.2 Importando sistemas de arquivos manualmente 664
42.3 Exportando sistemas de arquivos com o YaST 665
42.4 Exportando sistemas de arquivos manualmente 666

43 DHCP **669**

43.1 Configurando um servidor DHCP com o YaST 670
43.2 Pacotes de software DHCP 673
43.3 O dhcpd do servidor DHCP 673
43.4 Para obter mais informações 677

44 Sincronização de horário com xntp **679**

44.1 Configurando um cliente NTP com YaST 679
44.2 Configurando o xntp na rede 683
44.3 Configurando um relógio de referência local 683

45 LDAP—Um serviço de diretório **685**

45.1 LDAP versus NIS 687
45.2 Estrutura de uma árvore de diretórios LDAP 688
45.3 Configuração do servidor com slapd.conf 691
45.4 Tratamento de dados no diretório LDAP 696
45.5 O cliente LDAP do YaST 700
45.6 Configurando grupos e usuários LDAP no YaST 708
45.7 Para obter mais informações 709

46 O servidor Web do Apache **711**

46.1 Prefácio e terminologia 711
46.2 Instalação 713
46.3 Configuração 720
46.4 Hosts virtuais 737
46.5 Módulos do Apache 741
46.6 Segurança 753
46.7 Solução de problemas 754
46.8 Para obter mais informações 755

47 Sincronização de arquivos **759**

47.1 Software de sincronização de dados disponível 759
47.2 Determinando fatores para selecionar um programa. 762
47.3 Introdução ao Unison 766
47.4 Introdução ao CVS 768
47.5 Introdução ao Subversion 771
47.6 Introdução ao rsync 774
47.7 Introdução ao mailsync 776

48 Samba **781**

48.1 Configurando o servidor 783
48.2 Samba como servidor de login 787
48.3 Configurando um servidor Samba com o YaST 789
48.4 Configurando clientes 791
48.5 Otimização 792

Índice Remissivo **795**

Sobre este guia

Este manual oferece uma visão geral do SUSE Linux. Ele se destina principalmente a administradores de sistemas e usuários domésticos com conhecimentos básicos de administração de sistemas. Este manual apresenta uma seleção de aplicativos necessários na vida quotidiana e oferece descrições detalhadas de cenários de instalação e configuração avançadas.

Cenários de distribuição avançada
Informações sobre como distribuir o SUSE Linux em ambientes complexos.

Internet, Multimídia, Office e Gráficos
Visão geral dos principais aplicativos de que um usuário doméstico pode precisar.

Mobilidade
Informações básicas sobre computação móvel com o SUSE Linux e configuração das diversas opções de computação sem fio, gerenciamento de energia e gerenciamento de perfil.

Administração
Informações sobre segurança no SUSE Linux, controles de acesso a sistemas de arquivos e alguns importantes utilitários para administradores do Linux.

Sistema
Informações sobre o funcionamento dos componentes do sistema Linux e detalhes sobre sua interação.

Serviços
Informações sobre como configurar os diversos serviços de rede e de arquivos oferecidos pelo SUSE Linux.

1 Feedback

Queremos receber seus comentários e sugestões sobre este manual e sobre a documentação restante que acompanha este produto. Use a função Comentários do Usuário, situada na parte inferior de cada página da documentação online, ou vá até `http://www.novell.com/documentation/feedback.html` e digite seus comentários.

2 Documentação adicional

Há outros manuais disponíveis sobre o produto SUSE Linux: online em http://www.novell.com/documentation/ ou no sistema instalado em /usr/share/doc/manual/:

Inicialização
Este guia aborda os primeiros passos com o SUSE Linux. Uma versão online deste documento pode ser encontrada em http://www.novell.com/documentation/suse10/.

Guia de Instalação e Inicialização Rápida do Novell AppArmor Powered by Immunix 1.2
Este guia descreve o procedimento inicial de instalação do produto *AppArmor*. Uma versão online deste documento pode ser encontrada em http://www.novell.com/documentation/apparmor/.

Guia de Administração do Novell AppArmor Powered by Immunix 1.2
Este guia contém informações detalhadas sobre o uso do *AppArmor* em seu ambiente. Uma versão online deste documento pode ser encontrada em http://www.novell.com/documentation/apparmor/.

3 Convenções da documentação

As seguintes convenções tipográficas são usadas neste manual:

- /etc/passwd: nomes de arquivo e diretório
- *marcador*: substitua *marcador* pelo valor real
- PATH: a variável de ambiente PATH
- ls, --help: comandos, opções e parâmetros
- user: usuários ou grupos
- Alt, Alt + F1: uma tecla para pressionar ou uma combinação de teclas

- *Arquivo*, *Arquivo* → *Salvar Como*: itens de menu, botões
- *Pingüins dançando* (Capítulo Penguins (Pingüins), ↑*Referência*): Esta é uma referência a outro manual.

4 Reconhecimento

Os desenvolvedores do Linux estão voluntariamente empenhados com a promoção do desenvolvimento do Linux em escala global. Agradecemos por seus esforços — esta distribuição não seria possível sem eles. Ademais, gostaríamos de agradecer a Frank Zappa e a Pawar. Agradecimentos especiais, claro, a Linus Torvalds.

Divirta-se!

Equipe SUSE

Parte I Cenários de distribuição avançados

1 Instalação remota

O SUSE Linux pode ser instalado de várias maneiras. Como na instalação comum de CD ou DVD abordada no Chapter *Instalação com o YaST* (↑Inicialização), você pode escolher entre vários métodos baseados em rede ou até mesmo optar por um método totalmente sem intervenção para a instalação do SUSE Linux.

Cada método é apresentado por meio de duas listas de verificação breves: uma que relaciona os pré-requisitos do método e outra que ilustra o procedimento básico. São fornecidos mais detalhes para todas as técnicas usadas nos cenários de instalação.

NOTA

Nas seções a seguir, o sistema que manterá a instalação do seu novo SUSE Linux é conhecido como *sistema de destino* ou *destino de instalação*. O termo *fonte de instalação* é usado para todas as fontes de dados de instalação. Isso inclui mídia física, como CD e DVD e servidores de rede que distribuem os dados de instalação na sua rede.

1.1 Cenários de instalação para instalação remota

Esta seção apresenta os cenários de instalação mais comuns para instalações remotas. Para cada cenário, verifique cuidadosamente a lista de pré-requisitos e siga o procedimento descrito para este cenário. Se necessitar de instruções detalhadas para uma etapa específica, siga os links fornecidos para cada uma.

IMPORTANTE

A configuração do sistema X Window não faz parte de nenhum processo de instalação remota. Ao término da instalação, efetue login no sistema de destino como root, digite `init 3` e inicie SaX2 para configurar o hardware de vídeo, como descrito na Seção 35.1, “Configuração do X11 com o SaX2” (p 545).

1.1.1 Instalação remota simples por VNC: configuração de rede estática

Este tipo de instalação ainda requer algum grau de acesso físico ao sistema de destino para inicializar na instalação. A instalação em si é inteiramente controlada por uma estação de trabalho remota usando VNC para se conectar ao programa de instalação. A interação do usuário é necessária, como na instalação manual no Chapter *Instalação com o YaST* (↑Inicialização).

Para este tipo de instalação, verifique se os seguintes requisitos foram atendidos:

- Fonte da instalação remota: NFS, HTTP, FTP ou SMB com conexão de rede ativa
- Sistema de destino com conexão de rede ativa
- Sistema de controle com conexão de rede ativa e software visualizador VNC ou browser habilitado para Java (Firefox, Konqueror, Internet Explorer ou Opera)
- Mídia física de inicialização (CD ou DVD) para inicializar o sistema de destino
- Endereços IP estático válidos já atribuídos à fonte de instalação e ao sistema de controle
- Endereços IP estático válidos para atribuir ao sistema de destino

Para executar este tipo de instalação, proceda da seguinte maneira:

1. Configure a fonte de instalação como descrito na Seção 1.2, “Configurando o servidor que mantém as fontes de instalação” (p 30).
2. Inicialize o sistema de destino usando o primeiro CD ou DVD do kit de mídia do SUSE Linux.

3 Quando a tela de inicialização do sistema de destino for exibida, use o prompt de opções de inicialização para definir as opções de VNC apropriadas e o endereço da fonte de instalação. Isso está descrito detalhadamente na Seção 1.4, “Inicializando o sistema de destino para instalação” (p 50).

   O sistema de destino é inicializado em um ambiente baseado em texto, apresentando o endereço de rede e número de exibição sob o qual o ambiente de instalação gráfico pode ser endereçado por qualquer aplicativo visualizador VNC ou browser. As instalações VNC se anunciam em OpenSLP e podem ser encontradas usando-se o Konqueror no modo `service://` ou `slp://`.

4 Na estação de trabalho de controle, abra um aplicativo de visualização VNC ou browser da Web e conecte-se ao sistema de destino como descrito na Seção 1.5.1, “Instalação VNC” (p 55).

5 Execute a instalação como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

   Será necessário reconectar-se ao sistema de destino depois de reinicializado, para concluir a parte final da instalação.

6 Conclua a instalação.

1.1.2 Instalação remota simples por VNC: configuração de rede dinâmica por DHCP

Este tipo de instalação ainda requer algum grau de acesso físico ao sistema de destino para inicializar na instalação. A configuração de rede é feita com DHCP. A instalação em si é inteiramente controlada por uma estação de trabalho remota usando VNC para conectar-se ao instalador, mas ainda requer a interação do usuário no trabalho real de configuração.

Para este tipo de instalação, verifique se os seguintes requisitos foram atendidos:

- Fonte da instalação remota: NFS, HTTP, FTP ou SMB com conexão de rede ativa
- Sistema de destino com conexão de rede ativa

- Sistema de controle com conexão de rede ativa e software visualizador VNC ou browser habilitado para Java (Firefox, Konqueror, Internet Explorer ou Opera)
- Mídia física de inicialização (CD, DVD, disco de inicialização personalizado) para inicializar o sistema de destino
- Servidor DHCP em execução fornecendo endereços IP

Para executar este tipo de instalação, proceda da seguinte maneira:

1. Configure a fonte de instalação como descrito na Seção 1.2, “Configurando o servidor que mantém as fontes de instalação” (p 30). Escolha um servidor de rede NFS, HTTP ou FTP. No caso de uma fonte de instalação SMB, consulte a Seção 1.2.5, “Gerenciando uma fonte de instalação SMB” (p 39).

2. Inicialize o sistema de destino usando o primeiro CD ou DVD do kit de mídia do SUSE Linux.

3. Quando a tela de inicialização do sistema de destino for exibida, use o prompt de opções de inicialização para definir as opções de VNC apropriadas e o endereço da fonte de instalação. Isso está descrito detalhadamente na Seção 1.4, “Inicializando o sistema de destino para instalação” (p 50).

   O sistema de destino é inicializado em um ambiente baseado em texto, apresentando o endereço de rede e número de exibição sob o qual o ambiente de instalação gráfico pode ser endereçado por qualquer aplicativo visualizador VNC ou browser. As instalações VNC se anunciam em OpenSLP e podem ser encontradas usando-se o Konqueror no modo `service://` ou `slp://`.

4. Na estação de trabalho de controle, abra um aplicativo de visualização VNC ou browser da Web e conecte-se ao sistema de destino como descrito na Seção 1.5.1, “Instalação VNC” (p 55).

5. Execute a instalação como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

   Será necessário reconectar-se ao sistema de destino depois de reinicializado, para concluir a parte final da instalação.

6. Conclua a instalação.

1.1.3 Instalação remota por VNC: inicialização PXE e Wake on LAN

Este tipo de instalação ocorre totalmente sem intervenção. A máquina de destino é inicializada remotamente. A interação do usuário só é necessária para a instalação em si. Este método é adequado para distribuições entre sites.

Para executar este tipo de instalação, verifique se os seguintes requisitos foram atendidos:

- Fonte da instalação remota: NFS, HTTP, FTP ou SMB com conexão de rede ativa
- Servidor TFTP
- Servidor DHCP em execução para sua rede
- Sistema de destino com recurso de inicialização PXE, rede e Wake on LAN, conectado à rede
- Sistema de controle com conexão de rede ativa e software visualizador VNC ou browser habilitado para Java (Firefox, Konqueror, Internet Explorer ou Opera)

Para executar este tipo de instalação, proceda da seguinte maneira:

1. Configure a fonte de instalação como descrito na Seção 1.2, “Configurando o servidor que mantém as fontes de instalação” (p 30). Escolha um servidor de rede NFS, HTTP, FTP ou configure uma fonte de instalação SMB como descrito na Seção 1.2.5, “Gerenciando uma fonte de instalação SMB” (p 39).

2. Configure um servidor TFTP para manter uma imagem de inicialização que possa ser extraída pelo sistema de destino. Isso está descrito na Seção 1.3.2, “Configurando um servidor TFTP” (p 42).

3. Configure um servidor DHCP para fornecer endereços IP a todas as máquinas e revelar a localização do servidor TFTP para o sistema de destino. Isso está descrito na Seção 1.3.1, “Configurando um servidor DHCP” (p 40).

4. Prepare o sistema de destino para a inicialização PXE. Isso está descrito detalhadamente na Seção 1.3.5, “Preparando o sistema de destino para inicialização PXE” (p 48).

5 Inicie o processo de inicialização do sistema de destino usando Wake on LAN. Isso está descrito na Seção 1.3.7, “Wake on LAN” (p 49).

6 Na estação de trabalho de controle, abra um aplicativo de visualização VNC ou browser da Web e conecte-se ao sistema de destino como descrito na Seção 1.5.1, “Instalação VNC” (p 55).

7 Execute a instalação como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

   Será necessário reconectar-se ao sistema de destino depois de reinicializado, para concluir a parte final da instalação.

8 Conclua a instalação.

1.1.4 Instalação remota simples por SSH: configuração de rede estática

Este tipo de instalação ainda requer algum grau de acesso físico ao sistema de destino para a inicialização na instalação e para determinar o endereço IP do destino de instalação. A instalação em si é inteiramente controlada de uma estação de trabalho remota usando SSH para se conectar ao instalador. A interação do usuário é necessária, como na instalação comum descrita no Chapter *Instalação com o YaST* (↑Inicialização).

Para este tipo de instalação, verifique se os seguintes requisitos foram atendidos:

- Fonte da instalação remota: NFS, HTTP, FTP ou SMB com conexão de rede ativa
- Sistema de destino com conexão de rede ativa
- Sistema de controle com conexão de rede ativa e software visualizador VNC ou browser habilitado para Java (Firefox, Konqueror, Internet Explorer ou Opera)
- Mídia física de inicialização (CD, DVD, disco de inicialização personalizado) para o sistema de destino
- Endereços IP estático válidos já atribuídos à fonte de instalação e ao sistema de controle

- Endereços IP estático válidos para atribuir ao sistema de destino

Para executar este tipo de instalação, proceda da seguinte maneira:

1. Configure a fonte de instalação como descrito na Seção 1.2, “Configurando o servidor que mantém as fontes de instalação” (p 30).

2. Inicialize o sistema de destino usando o primeiro CD ou DVD do kit de mídia do SUSE Linux.

3. Quando a tela de inicialização do sistema de destino for exibida, use o prompt de opções de inicialização para definir os parâmetros apropriados de conexão de rede, o endereço da fonte de instalação e a habilitação SSH. Isso está descrito detalhadamente na Seção 1.4.3, “Usando opções de inicialização personalizadas” (p 52).

   O sistema de destino é inicializado em um ambiente baseado em texto, apresentando o endereço de rede e número de exibição sob o qual o ambiente de instalação gráfico pode ser endereçado por qualquer cliente SSH.

4. Na estação de trabalho de controle, abra uma janela de terminal e conecte-se ao sistema de destino como descrito na “Conectando-se ao programa de instalação” (p 57).

5. Execute a instalação como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

   Será necessário reconectar-se ao sistema de destino depois de reinicializado, para concluir a parte final da instalação.

6. Conclua a instalação.

1.1.5 Instalação remota simples por SSH: configuração de rede dinâmica por DHCP

Este tipo de instalação ainda requer algum grau de acesso físico ao sistema de destino para a inicialização na instalação e para determinar o endereço IP do destino de

instalação. A instalação em si é inteiramente controlada por uma estação de trabalho remota usando VNC para conectar-se ao instalador, mas ainda requer a interação do usuário no trabalho real de configuração.

Para este tipo de instalação, verifique se os seguintes requisitos foram atendidos:

- Fonte da instalação remota: NFS, HTTP, FTP ou SMB com conexão de rede ativa
- Sistema de destino com conexão de rede ativa
- Sistema de controle com conexão de rede ativa e software visualizador VNC ou browser habilitado para Java (Firefox, Konqueror, Internet Explorer ou Opera)
- Mídia física de inicialização (CD ou DVD) para inicializar o sistema de destino
- Servidor DHCP em execução fornecendo endereços IP

Para executar este tipo de instalação, proceda da seguinte maneira:

1. Configure a fonte de instalação como descrito na Seção 1.2, “Configurando o servidor que mantém as fontes de instalação” (p 30). Escolha um servidor de rede NFS, HTTP ou FTP. No caso de uma fonte de instalação SMB, consulte a Seção 1.2.5, “Gerenciando uma fonte de instalação SMB” (p 39).

2. Inicialize o sistema de destino usando o primeiro CD ou DVD do kit de mídia do SUSE Linux.

3. Quando a tela de inicialização do sistema de destino for exibida, use o prompt de opções de inicialização para passar os parâmetros apropriados de conexão de rede, a localização da fonte de instalação e a habilitação SSH. Consulte a Seção 1.4.3, “Usando opções de inicialização personalizadas” (p 52) para obter instruções detalhadas sobre o uso desses parâmetros.

   O sistema de destino é inicializado em um ambiente baseado em texto, apresentando o endereço de rede sob o qual o ambiente de instalação gráfica pode ser endereçado por qualquer cliente SSH.

4. Na estação de trabalho de controle, abra uma janela de terminal e conecte-se ao sistema de destino como descrito na “Conectando-se ao programa de instalação” (p 57).

5 Execute a instalação como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

   Será necessário reconectar-se ao sistema de destino depois de reinicializado, para concluir a parte final da instalação.

6 Conclua a instalação.

1.1.6 Instalação remota por SSH: inicialização PXE e Wake on LAN

Este tipo de instalação ocorre totalmente sem intervenção. A máquina de destino é inicializada remotamente.

Para executar este tipo de instalação, verifique se os seguintes requisitos foram atendidos:

- Fonte da instalação remota: NFS, HTTP, FTP ou SMB com conexão de rede ativa
- Servidor TFTP
- Servidor DHCP em execução para sua rede, fornecendo um IP estático para o host que precisa ser instalado
- Sistema de destino com recurso de inicialização PXE, rede e Wake on LAN, conectado à rede
- Sistema de controle com conexão de rede ativa e software cliente SSH

Para executar este tipo de instalação, proceda da seguinte maneira:

1 Configure a fonte de instalação como descrito na Seção 1.2, “Configurando o servidor que mantém as fontes de instalação” (p 30). Escolha um servidor de rede NFS, HTTP ou FTP. Para obter informações sobre como configurar uma fonte de instalação SMB, consulte a Seção 1.2.5, “Gerenciando uma fonte de instalação SMB” (p 39).

2 Configure um servidor TFTP para manter uma imagem de inicialização que possa ser extraída pelo sistema de destino. Isso está descrito na Seção 1.3.2, “Configurando um servidor TFTP” (p 42).

3 Configure um servidor DHCP para fornecer endereços IP a todas as máquinas e revelar a localização do servidor TFTP para o sistema de destino. Isso está descrito na Seção 1.3.1, “Configurando um servidor DHCP” (p 40).

4 Prepare o sistema de destino para a inicialização PXE. Isso está descrito detalhadamente na Seção 1.3.5, “Preparando o sistema de destino para inicialização PXE” (p 48).

5 Inicie o processo de inicialização do sistema de destino usando Wake on LAN. Isso está descrito na Seção 1.3.7, “Wake on LAN” (p 49).

6 Na estação de trabalho de controle, inicie um cliente VNC e conecte-se ao sistema de destino como descrito na Seção 1.5.2, “Instalação SSH” (p 57).

7 Execute a instalação como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

Será necessário reconectar-se ao sistema de destino depois de reinicializado, para concluir a parte final da instalação.

8 Conclua a instalação.

1.2 Configurando o servidor que mantém as fontes de instalação

Dependendo do sistema operacional executado na máquina a ser usada como fonte de instalação em rede para o SUSE Linux, há várias opções para a configuração do servidor. A maneira mais fácil de configurar um servidor de instalação é usar o YaST no SUSE LINUX Enterprise Server 9 ou SUSE Linux 9.3 e superior. Em outras versão do SUSE LINUX Enterprise Server ou do SUSE Linux, configure a fonte de instalação manualmente.

DICA

Você pode usar uma máquina Microsoft Windows como servidor de instalação para a distribuição do Linux. Consulte a Seção 1.2.5, “Gerenciando uma fonte de instalação SMB” (p 39) para obter detalhes.

1.2.1 Configurando um servidor de instalação usando YaST

O YaST oferece uma ferramenta gráfica para criar fontes de instalação em rede. Ele possui suporte a servidores de instalação em rede HTTP, FTP e NFS.

1. Efetue login como root na máquina que deverá atuar como servidor de instalação.

2. Inicie *YaST* → *Diversos* → *Servidor de Instalação*.

3. Selecione o tipo de servidor (HTTP, FTP ou NFS).

   O serviço de servidor selecionado é iniciado automaticamente toda vez que o sistema inicializa. Se um serviço do tipo selecionado já estiver em execução no seu sistema e você quiser configurá-lo manualmente para o servidor, desative a configuração automática do serviço de servidor com *Não configure serviços de rede*. Em ambos os casos, defina o diretório em que os dados da instalação devem estar disponíveis no servidor.

4. Configure o tipo de servidor necessário.

   Esta etapa refere-se à configuração automática dos serviços de servidor. Ela é ignorada quando a configuração automática está desativada. Defina um álias para o diretório raiz do servidor FTP ou HTTP no qual os dados de instalação devem ser encontrados. A fonte de instalação posteriormente estará localizada em `ftp://IP do servidor/Álias/Nome` (FTP) ou em `http://IP do servidor/Álias/Nome` (HTTP). *Nome* significa o nome da fonte de instalação, que é definida na etapa seguinte. Se você selecionou NFS na etapa anterior, defina curingas e opções de exportações. O servidor NFS estará disponível em `nfs://IP do servidor/Nome`. Detalhes sobre NFS e exportações são encontrados no Capítulo 42, *Compartilhando sistemas de arquivos com o NFS* (p 663).

5. Configure a fonte de instalação.

   Antes que as mídias de instalação sejam copiadas para seu destino, defina o nome da fonte de instalação (de preferência, uma abreviação fácil de ser lembrada do produto e da versão). O YaST permite fornecer imagens ISO da mídia em vez de cópias dos CDs de instalação. Se desejar, ative a caixa de seleção relevante e

especifique o caminho de diretório no qual os arquivos ISO podem ser encontrados localmente. Dependendo do produto a distribuir usando este servidor de instalação, talvez sejam necessários mais CDs de expansão ou CDs de service pack para instalar o produto completamente. Se você ativar *Solicitar CDs adicionais*, o YaST o lembrará automaticamente de fornecer essas mídias. Para anunciar o servidor de instalação na rede por OpenSLP, ative a opção adequada.

DICA

Considere anunciar a sua fonte de instalação por OpenSLP se a sua configuração de rede for compatível com esta opção. Isto o livra de digitar o caminho de instalação da rede em todas as máquinas de destino. Os sistemas de destino, inicializados com a opção de inicialização SLP, encontrarão a fonte de instalação de rede sem outras configurações. Para obter detalhes sobre esta opção, consulte a Seção 1.4, “Inicializando o sistema de destino para instalação” (p 50).

---

6 Faça o upload dos dados de instalação.

A etapa mais longa da configuração de um servidor de instalação é copiar os CDs de instalação. Insira a mídia na seqüência solicitada pelo YaST e aguarde o término do procedimento de cópia. Quando as fontes tiverem sido completamente copiadas, volte para a visão geral das fontes de informações existentes e feche a configuração selecionando *Concluir*.

O seu servidor de instalação agora está totalmente configurado e pronto para serviço. Ele é inicializado automaticamente toda vez que o sistema é iniciado. Nenhuma outra intervenção é necessária. Você precisa apenas configurar e inicializar este serviço de forma correta e manualmente se tiver desativado a configuração automática do serviço de rede selecionado com YaST como etapa inicial.

Para desativar uma fonte de instalação, selecione *Mudar* na visão geral para chegar a uma lista de todas as fontes de instalação disponíveis. Escolha a entrada para remover e selecione *Apagar*. Este procedimento de exclusão só diz respeito à desativação do serviço de servidor. Os dados de instalação em si permanecem no diretório escolhido. No entanto, você pode removê-lo manualmente.

Se o seu servidor de instalação fornecer os dados de instalação para mais de um produto da versão de produto, inicie o módulo de servidor de instalação YaST e selecione

Configurar na visão geral das fontes de instalação existentes para configurar a nova fonte de instalação.

1.2.2 Configuração manual de uma fonte de instalação NFS

A configuração de uma fonte NFS para instalação é feita basicamente em duas etapas. Na primeira etapa, crie a estrutura de diretório que manterá os dados de instalação e copie a mídia de instalação nessa estrutura. Em seguida, exporte o diretório que manterá os dados de instalação para a rede.

Para criar um diretório para manter os dados de instalação, proceda da seguinte maneira:

1. Efetue login como root.

2. Crie um diretório que posteriormente manterá todos os dados de instalações e vá até ele. Por exemplo:

   ```
   mkdir install/produto/versão_do_produto
   cd install/produto/versão_do_produto
   ```

   Substitua *produto* por uma abreviação do nome do produto (neste caso, SUSE Linux) e *versão_do_produto* por uma string que contenha o nome e a versão do produto.

3. Para cada CD contido no kit de mídia, execute os seguintes comandos:

   a. Copie todo o conteúdo do CD de instalação para o diretório do servidor de instalação:

      ```
      cp -a /media/caminho_unidade_de_CD-ROM .
      ```

      Substitua *caminho_unidade_de_CD-ROM* pelo caminho real no qual está endereçada sua unidade de CD ou DVD. Dependendo do tipo de unidade usado no seu sistema, as opções são `cdrom`, `cdrecorder`, `dvd` ou `dvdrecorder`.

   b. Renomeie o diretório com o número do CD:

      ```
      mv caminho_unidade_de_CD-ROM CDx
      ```

Substitua *x* pelo número real do seu CD.

Para exportar as fontes de instalação por NFS usando YaST, proceda da seguinte maneira:

1. Efetue login como root.
2. Inicie *YaST → Serviços de Rede → Servidor NFS*.
3. Selecione *Iniciar Servidor NFS* e *Abrir Porta no Firewall* e clique em *Próximo*.
4. Selecione *Adicionar Diretório* e digite o caminho do diretório que mantém os dados de instalação. Neste caso, é `/versão_do_produto`.
5. Selecione *Adicionar Host* e digite os nomes de host das máquinas para as quais exportar os dados de instalação. Em vez de especificar os nomes de host aqui, você pode usar curingas, faixas de endereços de rede ou apenas o nome de domínio da sua rede. Digite as opções de exportação adequadas ou mantenha o padrão, que funciona bem na maioria das configurações. Para obter mais informações sobre a sintaxe usada na exportação de compartilhamentos NFS, leia a página de manual sobre `export` .
6. Clique em *Concluir*.

   O servidor NFS que mantém as fontes de instalação do SUSE Linux é inicializado automaticamente e integrado ao processo de inicialização.

Se você preferir exportar manualmente as fontes de instalação por NFS em vez de usar o módulo de servidor NFS do YaST, proceda da seguinte maneira:

1. Efetue login como root.
2. Abra o arquivo `/etc/exports` e digite a seguinte linha:

   ```
   /versão_do_produto *(ro,root_squash,sync)
   ```

   Isso exporta o diretório `/versão_do_produto` para qualquer host que faça parte desta rede ou para qualquer host que possa se conectar com este servidor. Para limitar o acesso a este servidor, use máscaras de rede ou nomes de domínio em vez do curinga geral `*`. Consulte a página de manual sobre `export` para obter detalhes. Grave e saia deste arquivo de configuração.

3 Para adicionar o serviço NFS à lista de servidores iniciados durante a inicialização do sistema, execute os seguintes comandos:

```
insserv /etc/init.d/nfsserver
```

```
insserv /etc/init.d/portmap
```

4 Inicie o servidor NFS usando o seguinte comando:

```
rcnfsserver start
```

Se você precisar mudar a configuração do seu servidor NFS posteriormente, modifique o arquivo de configuração e reinicie o daemon NFS com `rcnfsserver restart`.

Anunciar o servidor NFS por OpenSLP faz o seu endereço ser conhecido por todos os clientes da sua rede.

1 Efetue login como root.

2 Digite o diretório `/etc/slp.reg.d/`.

3 Crie um arquivo de configuração chamado `install.suse.nfs.reg` contendo as seguintes linhas:

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/caminho_fonte_inst/CD1,en,65535
description=NFS Installation Source
```

Substitua *`caminho_fonte_inst`* pelo caminho real da fonte de instalação no seu servidor.

4 Grave este arquivo de configuração e inicie o daemon OpenSLP usando o seguinte comando:

```
rcslpd start
```

Para obter mais informações sobre OpenSLP, consulte a documentação do pacote localizada em `/usr/share/doc/packages/openslp/` ou consulte o Capítulo 39, *Serviços SLP na rede* (p 629).

1.2.3 Configuração manual de uma fonte de instalação FTP

Criar uma fonte de instalação FTP é muito semelhante à criação de uma fonte de instalação NFS. As fontes de instalação FTP podem ser anunciadas na rede também usando OpenSLP.

1. Crie um diretório que mantenha as fontes de instalação conforme descrito na Seção 1.2.2, “Configuração manual de uma fonte de instalação NFS” (p 33).

2. Configure o servidor FTP para distribuir o conteúdo do seu diretório de instalação:

   a. Efetue login como root e instale o pacote `pure-ftpd` (um servidor FTP simples) usando o gerenciador de pacotes do YaST.

   b. Digite o diretório raiz do servidor FTP:

      ```
      cd/srv/ftp
      ```

   c. Crie um subdiretório que mantenha as fontes de instalação no diretório raiz do FTP:

      ```
      mkdirfonte_inst
      ```

      Substitua *`fonte_inst`* pelo nome do produto.

   d. Copie o conteúdo de todos os CDs de instalação no diretório raiz do servidor FTP (semelhante ao procedimento descrito na Seção 1.2.2, “Configuração manual de uma fonte de instalação NFS” (p 33), Passo 3 (p 33)).

      Como alternativa, monte o conteúdo do repositório de instalação já existente no ambiente raiz de mudanças do servidor FTP:

      ```
      mount --bind
      caminho_fonte_inst /srv/ftp/fonte_inst
      ```

Substitua *caminho_fonte_inst* e *fonte_inst* pelos valores correspondentes à sua configuração. Se precisar tornar os valores permanentes, adicione-os a `/etc/fstab`.

e Inicie pure-ftpd:

```
pure-ftpd &
```

3 Anuncie a fonte de instalação por OpenSLP, se for suportado pela configuração da sua rede:

a Crie um arquivo de configuração chamado `install.suse.ftp.reg` em `/etc/slp/reg.d/` com as seguintes linhas:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/fonte_inst/CD1,en,65535
description=FTP Installation Source
```

Substitua *fonte_inst* pelo nome real no diretório da fonte de instalação do seu servidor. A linha `service:` deve ser digitada como uma linha contínua.

b Grave este arquivo de configuração e inicie o daemon OpenSLP usando o seguinte comando:

```
rcslpd start
```

1.2.4 Configuração manual de uma fonte de instalação HTTP

Criar uma fonte de instalação HTTP é muito semelhante à criação de uma fonte de instalação NFS. As fontes de instalação HTTP podem ser anunciadas na rede também usando OpenSLP.

1 Crie um diretório que mantenha as fontes de instalação conforme descrito na Seção 1.2.2, “Configuração manual de uma fonte de instalação NFS” (p 33).

2 Configure o servidor HTTP para distribuir o conteúdo do seu diretório de instalação:

a Efetue login como root e instale o pacote `apache2` usando o gerenciador de pacotes do YaST.

b Digite o diretório raiz do servidor HTTP (`/srv/www/htdocs`) e crie um subdiretório que manterá as fontes de instalação:

```
mkdir fonte_inst
```

Substitua *`fonte_inst`* pelo nome do produto.

c Crie um link simbólico do local das fontes de instalação para o diretório raiz do servidor Web (`/srv/www/htdocs`):

```
ln -s /caminho_fonte_inst /srv/www/htdocs/fonte_inst
```

d Modifique o arquivo de configuração do servidor HTTP (`/etc/apache2/default-server.conf`) para fazê-lo seguir links simbólicos. Substitua a seguinte linha:

```
Options None
```

por

```
Options Indexes FollowSymLinks
```

e Reinicie o servidor HTTP usando `rcapache2 restart`.

3 Anuncie a fonte de instalação por OpenSLP, se for suportado pela configuração da sua rede:

a Crie um arquivo de configuração chamado `install.suse.http.reg` em `/etc/slp/reg.d/` com as seguintes linhas:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/caminho_fonte_inst/CD1/,en,65535
description=HTTP Installation Source
```

Substitua *`caminho_fonte_inst`* pelo caminho real da fonte de instalação no seu servidor. A linha `service:` deve ser digitada como uma linha contínua.

b Grave este arquivo de configuração e inicie o daemon OpenSLP usando `rcslpd restart`.

1.2.5 Gerenciando uma fonte de instalação SMB

Com o SMB (Samba), é possível importar as fontes de instalação de um servidor Microsoft Windows e iniciar a distribuição do Linux mesmo sem nenhuma máquina Linux.

Para configurar um Compartilhamento Windows exportado mantendo as suas fontes de instalação do SUSE Linux, proceda da seguinte maneira:

1. Efetue login na sua máquina Windows.
2. Inicie o Explorer e crie uma nova pasta que manterá toda a árvore de instalação e denomine-a `INSTALAR`, por exemplo.
3. Exporte este compartilhamento de acordo com o procedimento descrito na sua documentação do Windows.
4. Digite este compartilhamento e crie uma subpasta, denominada *`produto`*. *`produto`* deve ser substituído pelo nome real do produto (SUSE Linux neste caso).
5. Copie cada CD do SUSE Linux em uma pasta separada e denomine essas pastas `CD1`, `CD2`, `CD3` etc.
6. Digite o diretório superior do compartilhamento exportado (`INSTALAR`, neste exemplo) e copie os seguintes arquivos de *`produto`*`/CD1` para esta pasta: `content`, `media.1`, `control.xml` e `boot`.
7. Crie uma nova pasta em `INSTALAR` e denomine-a `yast`.
8. Digite a pasta `yast` e crie os arquivos `order` e `instorder`.
9. Abra o arquivo `order` e digite a seguinte linha:

   ```
   /NLD/CD1 smb://usu rio:senha@nome_do_host/produtoCD1
   ```

   Substitua *`usuário`* pelo nome de usuário que você usa na máquina Windows ou use `Guest` para habilitar o login de convidado a este compartilhamento. *`senha`* deve ser substituído por sua senha de login ou qualquer outra string para

login de convidado. *nome_do_host* deve ser substituído pelo nome de rede da sua máquina Windows.

- Abra o arquivo `instorder` e digite a seguinte linha:

  `/produto/CD1`

Para usar um compartilhamento SMB montado como fonte de instalação, proceda da seguinte maneira:

1. Inicialize o destino de instalação.
2. Selecione *Instalação*.
3. Pressione F4 para obter uma seleção de fontes de instalação.
4. Escolha SMB e digite o nome ou endereço IP da máquina Windows, o nome de compartilhamento (`INSTALAR`, neste exemplo), nome de usuário e senha.

   Depois que você pressionar Enter, o YaST será iniciado e você poderá executar a instalação.

1.3 Preparando a inicialização do sistema de destino

Esta seção aborda as tarefas de configuração necessárias em cenários complexos de inicialização. Contém exemplos de configurações prontas para aplicar referentes a DHCP, inicialização PXE, TFTP e Wake on LAN.

1.3.1 Configurando um servidor DHCP

A configuração de um servidor DHCP em SUSE Linux é feita editando-se manualmente os arquivos de configuração apropriados. Esta seção aborda a extensão de configuração de um servidor DHCP existente visando fornecer os dados necessários para atender um ambiente TFTP, PXE e WOL.

Configuração manual de um servidor DHCP

Tudo o que o servidor DHCP deve fazer, além de fornecer alocação de endereço automática para os seus clientes de rede, é anunciar o endereço IP do servidor TFTP e o arquivo que deve ser extraído pelas rotinas de instalação na máquina de destino.

1. Efetue login como root na máquina que hospeda o servidor DHCP.

2. Anexe as linhas seguintes ao arquivo de configuração do seu servidor DHCP localizado em `/etc/dhcpd.conf`:

   ```
   group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_servidor_tftp:
    #
    # "filename" specifiies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename  "pxelinux.0";
   }
   ```

   Substitua *`ip_servidor_tftp`* pelo endereço IP real do servidor TFTP.

   Para obter mais informações sobre as opções disponíveis em `dhcpd.conf`, consulte a página de manual sobre `dhcpd.conf`.

3. Reinicie o servidor DHCP executando `rcdhcpd restart`

Se você planeja usar SSH para controle remoto de uma instalação PXE e Wake on LAN, especifique explicitamente o endereço IP que o DHCP deve fornecer ao destino de instalação. Para isso, modifique a configuração DHCP mencionada acima de acordo com o exemplo a seguir:

```
group {
 # PXE related stuff
 #
 # "next server" defines the tftp server that will be used
 next server ip_servidor_tftp:
 #
 # "filename" specifiies the pxelinux image on the tftp server
 # the server runs in chroot under /srv/tftpboot
 filename "pxelinux.0";
 host test { hardware ethernet endereço_mac;
    fixed-address um_endereço_ip; }
  }
```

A declaração de host apresenta o nome de host do destino de instalação. Para vincular o nome de host e o endereço IP a um host específico, você precisa conhecer e especificar o endereço de hardware do sistema (MAC). Substitua todas as variáveis usadas neste exemplo pelos valores reais que correspondem ao seu ambiente.

Após a reinicialização do servidor DHCP, ele fornece um IP estático para o host especificado, habilitando-o a conectar-se ao sistema por SSH.

1.3.2 Configurando um servidor TFTP

A configuração de um servidor TFTP pode ser feita com YaST ou manualmente em qualquer outro sistema operacional Linux que tenha suporte a xinetd e tftp. O servidor TFTP fornece a imagem de inicialização para o sistema de destino uma vez que inicializa e envia uma solicitação ao mesmo.

Configurando um servidor TFTP usando YaST

1. Efetue login como root.
2. Inicie *YaST → Serviços de Rede → Servidor TFTP* e instale o pacote solicitado.
3. Clique em *Habilitar* para verificar se o servidor foi iniciado e incluído nas rotinas de inicialização. De sua parte, não é necessária nenhuma outra ação de proteção. O xinetd inicia o tftpd no momento de inicialização.
4. Clique em *Abrir Porta no Firewall* para abrir a porta adequada no firewall em execução na sua máquina. Se nenhum firewall estiver em execução no seu servidor, esta opção não está disponível.
5. Clique em *Pesquisar* para pesquisar o diretório de imagem de inicialização.

   O diretório padrão `/tftpboot` é criado e selecionado automaticamente.
6. Clique em *Concluir* para aplicar as suas configurações e iniciar o servidor.

Configuração manual de um servidor TFTP

1. Efetue login como root e instale os pacotes `tftp` e `xinetd`.

2 Se indisponível, crie os diretórios `/srv/tftpboot` e `/srv/tftpboot/pxelinux.cfg`.

3 Adicione os arquivos adequados para a imagem de inicialização conforme descrito na Seção 1.3.3, “Inicialização PXE” (p 43).

4 Modifique a configuração de xinetd localizada em `/etc/xinetd.d/` para verificar se o servidor TFTP é iniciado durante a inicialização:

   a Se não existir, crie um arquivo chamado `tftp` neste diretório com `touch tftp`. Em seguida, execute `chmod 755 tftp`.

   b Abra o arquivo `tftp` e adicione as seguintes linhas:

```
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
        disable                 = no
}
```

   c Grave o arquivo e reinicie xinetd com `rcxinetd restart`.

1.3.3 Inicialização PXE

Informações técnicas e especificações completas sobre PXE estão disponíveis no documento Preboot Execution Environment (PXE) Specification (`ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf`).

1 Vá até o diretório do seu repositório de instalação e copie os arquivos `linux`, `initrd`, `message` e `memtest` para o diretório `/srv/tftpboot` digitando o seguinte:

```
cp -a boot/loader/linux boot/loader/initrd
      boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Instale o pacote `syslinux` diretamente dos seus CDs ou DVDs de instalação com YaST.

3 Copie o arquivo `/usr/share/syslinux/pxelinux.0` para o diretório `/srv/tftpboot` digitando o seguinte:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Vá até o diretório do seu repositório de instalação e copie o arquivo `isolinux.cfg` para `/srv/tftpboot/pxelinux.cfg/default` digitando o seguinte:

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

5 Edite o arquivo `/srv/tftpboot/pxelinux.cfg/default` e remova as linhas que começam com `gfxboot`, `readinfo` e `framebuffer`.

6 Insira as seguintes entradas nas linhas anexas dos rótulos padrão `failsafe` e `apic`:

`insmod=e100`
Por meio desta entrada, o módulo de kernel para uma placa de rede Intel 100MBit/s é carregado nos clientes PXE. Esta entrada depende do hardware do cliente e deve ser adaptada de acordo. No caso de uma placa de rede Broadcom GigaBit, esta entrada deve indicar `insmod=bcm5700`.

`netdevice=eth0`
Esta entrada define a interface de rede do cliente que deve ser usada para a instalação da rede. Só será necessária se o cliente possuir várias placas de rede, devendo ser adaptada de acordo. No caso de uma única placa de rede, esta entrada pode ser omitida.

`install=nfs://`*`ip_servidor_inst`*`/`*`caminho_fonte_inst`*`/CD1`
Esta entrada define o servidor NFS e a fonte de instalação para a instalação do cliente. Substitua *`ip_servidor_inst`* pelo endereço IP real do seu servidor de instalação. *`caminho_fonte_inst`* deve ser substituído pelo caminho real para as fontes de instalação. As fontes HTTP, FTP ou SMB são endereçadas de maneira semelhante, exceto pelo prefixo de protocolo, que deve indicar `http`, `ftp` ou `smb`.

IMPORTANTE

Se precisar passar outras opções de inicialização para as rotinas de instalação, como parâmetros de inicialização SSH ou VNC, anexe-os

à entrada `install`. Uma visão geral dos parâmetros e alguns exemplos são apresentados na Seção 1.4, “Inicializando o sistema de destino para instalação” (p 50).

A seguir, temos um exemplo de arquivo `/srv/tftpboot/pxelinux.cfg/default`. Ajuste o prefixo de protocolo para a fonte de instalação para corresponder à configuração da sua rede e especifique o seu método de conexão preferido para o instalador adicionando as opções `vnc` e `vncpassword` ou `ssh` e `sshpassword` à entrada `install`. As linhas separadas por `\` devem ser digitadas como uma linha contínua sem quebra de linha e sem `\`.

```
default linux

# default
label linux
  kernel linux
     append initrd=initrd ramdisk_size=65536 insmod=e100 \
     install=nfs://ip_servidor_inst/caminho_fonte_inst/produto

# failsafe
label failsafe
  kernel linux append initrd=initrd ramdisk_size=65536 ide=nodma apm=off
 acpi=off \ insmod=e100
   install=nfs://ip_servidor_inst/caminho_fonte_inst/produto

# apic
label apic
  kernel linux
  append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
  install=nfs://ip_servidor_inst/caminho_fonte_inst/produto

# manual
label manual
  kernel linux
  append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
  kernel linux
  append initrd=initrd ramdisk_size=65536 rescue=1

#  memory test
label memtest
  kernel memtest

# hard disk
label harddisk
  kernel linux append SLX=0x202
```

```
implicit     0
display      message
prompt       1
timeout      100
```

Substitua *ip_servidor_inst* e *caminho_fonte_inst* pelos valores usados na sua configuração.

A seção a seguir serve como breve referência às opções PXELINUX usadas nesta configuração. Mais informações sobre as opções disponíveis são encontradas na documentação do pacote `syslinux` localizada em `/usr/share/doc/packages/syslinux/`.

1.3.4 Opções de configuração PXELINUX

As opções relacionadas aqui são um subconjunto de todas as opções disponíveis para o arquivo de configuração PXELINUX.

DEFAULT *opções de kernel...*
Configura a linha de comando padrão do kernel. Se PXELINUX é inicializado automaticamente, atua como se as entradas após DEFAULT tivessem sido digitadas no prompt de inicialização, exceto a opção auto, que é adicionada automaticamente, indicando uma inicialização automática.

Se nenhum arquivo de configuração ou nenhuma entrada DEFAULT estiver presente no arquivo de configuração, o padrão será o nome de kernel "linux" sem opções.

APPEND *opções...*
Adicione uma ou mais opções à linha de comando do kernel. São adicionadas para inicializações manuais e automáticas. As opções são adicionadas no início da linha de comando do kernel, normalmente permitindo que as opções de kernel digitadas explicitamente as substituam.

LABEL *rótulo* KERNEL *imagem* APPEND *opções...*
Indica que se *rótulo* for digitado como kernel de inicialização, PXELINUX deve, por sua vez, inicializar *imagem*, e as opções `APPEND` especificadas devem ser usadas em vez das que estão especificadas na seção global do arquivo (antes do primeiro comando `LABEL`). O padrão para *imagem* é o mesmo de *rótulo* e, se não for fornecido nenhum `APPEND`, o padrão será usar a entrada global (se houver). Até 128 entradas `LABEL` são permitidas.

Observe que GRUB usa a seguinte sintaxe:

```
title meutítulo
  kernel meu_kernel opções_kernel
  initrd meuinitrd
```

enquanto que PXELINUX usa a seguinte sintaxe:

```
label meurótulo
  kernel meukernel
  append minhasopções
```

Os rótulos são desmembrados como se fossem nomes de arquivo e devem ser exclusivos após o desmembramento. Por exemplo, não seria possível distinguir os dois rótulos "v2.1.30" e "v2.1.31" em PXELINUX, pois ambos são desmembrados em um mesmo nome de arquivo do DOS.

O kernel não tem precisa ser um kernel do Linux; pode ser um setor de inicialização ou um arquivo COMBOOT.

APPEND -

Não anexa nada. `APPEND` com um único hífen como argumento em uma seção `LABEL` pode ser usado para anular um `APPEND` global.

`LOCALBOOT` *`tipo`*

Em PXELINUX, especificar `LOCALBOOT 0` em vez de uma opção `KERNEL` significa chamar este rótulo específico e causa uma inicialização de disco local em vez de uma inicialização de kernel.

Argumento	Descrição
`0`	Executa uma inicialização normal
`4`	Executa uma inicialização local com o driver UNDI (Universal Network Driver Interface) ainda residente na memória
`5`	Realiza uma inicialização local com toda a pilha PXE, incluindo o driver UNDI, ainda residente na memória

Todos os outros valores são indefinidos. Se você não sabe quais são as pilhas UNDI ou PXE, especifique `0`.

`TIMEOUT` *`tempo_de_espera`*

Indica quanto tempo esperar no prompt de inicialização até inicializar automaticamente, em unidades de 1/10 de segundo. O tempo de espera é cancelado tão logo o usuário digite algo no teclado, partindo do princípio de que o usuário conclui o comando iniciado. O tempo de espera zero desabilita completamente o tempo de espera (que é também o padrão).

O valor do tempo de espera máximo possível é 35996 (pouco menos de uma hora).

`PROMPT` *`val_flag`*

Se `val_flag` for 0, só exibirá o prompt de inicialização se Shift ou Alt estiver pressionado ou Caps Lock ou Scroll Lock estiver definido (que é o padrão). Se `val_flag` for 1, exibirá sempre o prompt de inicialização.

```
F2  nome_do_arquivo
F1  nome_do_arquivo
..etc...
F9  nome_do_arquivo
F10nome_do_arquivo
```

Exibe o arquivo indicado na tela quando uma tecla de função é pressionada no prompt de inicialização. Isso pode ser usado para implementar a ajuda online de pré-inicialização (supostamente para as opções de linha do comando do kernel). Para compatibilidade com versões anteriores, F10 também pode ser digitado como F0. Observe que atualmente não há meio de vincular nomes de arquivo a F11 e F12.

1.3.5 Preparando o sistema de destino para inicialização PXE

Prepare o BIOS do sistema para a inicialização PXE incluindo a opção PXE na ordem de inicialização do BIOS.

ATENÇÃO

Não coloque a opção PXE na frente da opção de inicialização do disco rígido no BIOS. Caso contrário, este sistema tentará reinstalar-se toda vez que você o inicializar.

1.3.6 Preparando o sistema de destino para Wake on LAN

Wake on LAN (WOL) requer que a opção de BIOS adequada seja habilitada antes da instalação. Além disso, anote o endereço MAC do sistema de destino. Esses dados são necessários para iniciar o Wake on LAN.

1.3.7 Wake on LAN

Wake on LAN permite que a máquina seja ligada por um pacote de rede especial que contém o endereço MAC da máquina. Como toda máquina no mundo tem um identificador MAC exclusivo, você não precisa se preocupar em ligar acidentalmente a máquina errada.

IMPORTANTE

Se a máquina controladora não estiver localizada no mesmo segmento de rede que o destino de instalação que deve ser desperto, configure as solicitações WOL para serem enviadas como multicasts ou controle remotamente uma máquina naquele segmento de rede para atuar como remetente das solicitações.

1.3.8 Wake on LAN manual

1. Efetue login como root.
2. Inicie *YaST → Instalar e Remover Software* e instale o pacote `netdiag`.

3 Abra um terminal e digite os seguintes comandos como root para despertar o destino:

```
ether-wakemac_do_destino
```

Substitua *mac_do_destino* pelo endereço MAC real do destino.

1.4 Inicializando o sistema de destino para instalação

Basicamente, há duas maneiras diferentes de personalizar o processo de inicialização para instalação, além das mencionadas na Seção 1.3.7, “Wake on LAN” (p 49) e na Seção 1.3.3, “Inicialização PXE” (p 43). Você pode usar as opções de inicialização padrão e as teclas F ou usar o prompt de opções da tela de inicialização da instalação para passar quaisquer opções de inicialização que o kernel de instalação possa precisar neste hardware específico.

1.4.1 Usando as opções padrão de inicialização

As opções de inicialização já foram descritas detalhadamente no Chapter *Instalação com o YaST* (↑Inicialização).

Geralmente, basta selecionar *Instalação* para iniciar o processo de inicialização de instalação. Se houver problemas, as opções *Instalação — ACPI Desabilitada* ou *Instalação — Configurações Seguras* podem ser úteis.

Para obter mais informações sobre solução de problemas no processo de instalação, consulte a Seção “Problemas de instalação” (Capítulo 9, *Problemas comuns e suas soluções*, ↑Inicialização).

1.4.2 Usando as teclas F

A barra de menus na tela inferior oferece algumas funcionalidades avançadas necessárias em algumas configurações. Usando as teclas F, você pode especificar opções adicionais para passar as rotinas de instalação sem conhecer a sintaxe detalhada dos parâmetros

que você precisaria se os inserisse como opções de inicialização (consulte a Seção 1.4.3, “Usando opções de inicialização personalizadas” (p 52)).

Consulte na tabela abaixo o conjunto completo das opções disponíveis.

Tabela 1.1 *Teclas F durante a instalação*

Tecla	Objetivo	Opções disponíveis	Valor padrão
F1	Fornecer ajuda	Nenhuma	Nenhum
F2	Selecionar o idioma da instalação	Todos os idiomas suportados	Inglês
F3	Mudar a resolução de tela para instalação	• Modo de texto • VESA • resolução 1 • resolução 2 • ...	• O valor padrão depende do seu hardware de vídeo
F4	Selecionar a fonte de instalação	• CD-ROM/DVD • SLP • FTP • HTTP • NFS • SMB • Disco rígido	CD-ROM/DVD

Tecla	Objetivo	Opções disponíveis	Valor padrão
F5	Aplicar disco de atualização do driver	Driver	Nenhum

1.4.3 Usando opções de inicialização personalizadas

Usar o conjunto adequado de opções de inicialização facilita o procedimento de instalação. Vários parâmetros também podem ser configurados posteriormente usando as rotinas linuxrc, mas usar as opções de inicialização é mais fácil. Em algumas configurações automatizadas, as opções de inicialização podem ser fornecidas com `initrd` ou um arquivo `info`.

A tabela a seguir relaciona todos os cenários de instalação mencionados neste capítulo com os parâmetros necessários para inicialização e as opções de inicialização correspondentes. Basta anexar todos eles na ordem em que aparecem nesta tabela para obter uma string de opção de inicialização que é passada para as rotinas de instalação. Por exemplo (todos em uma linha):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Substitua todos os valores (...) nesta string pelos valores adequados para a sua configuração.

Tabela 1.2 *Cenários de instalação (inicialização) usados neste capítulo*

Cenário de instalação	Parâmetros necessários para inicialização	Opções de inicialização
Chapter *Instalação com o YaST* (↑Inicialização)	Nenhum: o sistema é inicializado automaticamente	Nenhuma é necessária

Cenário de instalação	Parâmetros necessários para inicialização	Opções de inicialização
Seção 1.1.1, “Instalação remota simples por VNC: configuração de rede estática” (p 22)	• Localização do servidor de instalação • Dispositivo de rede • Endereço IP • Máscara de rede • Gateway • Habilitação VNC • Senha VNC	• `install=(nfs,http,ftp,smb)://caminho_mídia_inst` • `netdevice=um_disp_rede` (necessário apenas se vários dispositivos de rede estiverem disponíveis) • `hostip=um_ip` • `netmask=uma_máscara_rede` • `gateway=gateway_ip` • `vnc=1` • `vncpassword=uma_senha`
Seção 1.1.2, “Instalação remota simples por VNC: configuração de rede dinâmica por DHCP” (p 23)	• Localização do servidor de instalação • Habilitação VNC • Senha VNC	• `install=(nfs,http,ftp,smb)://caminho_mídia_inst` • `vnc=1` • `vncpassword=uma_senha`
Seção 1.1.3, “Instalação remota por VNC: inicialização PXE e Wake on LAN” (p 25)	• Localização do servidor de instalação • Localização do servidor TFTP • Habilitação VNC • Senha VNC	Não aplicável; processo gerenciado via PXE e DHCP

Cenário de instalação	Parâmetros necessários para inicialização	Opções de inicialização
Seção 1.1.4, “Instalação remota simples por SSH: configuração de rede estática” (p 26)	• Localização do servidor de instalação • Dispositivo de rede • Endereço IP • Máscara de rede • Gateway • Habilitação SSH • Senha SSH	• `install=(nfs,http,ftp,smb)://`*`caminho_mídia_inst`* • `netdevice=`*`um_disp_rede`* (necessário apenas se vários dispositivos de rede estiverem disponíveis) • `hostip=`*`um_ip`* • `netmask=`*`uma_máscara_rede`* • `gateway=`*`gateway_ip`* • `usessh=1` • `sshpassword=`*`uma_senha`*
Seção 1.1.5, “Instalação remota simples por SSH: configuração de rede dinâmica por DHCP” (p 27)	• Localização do servidor de instalação • Habilitação SSH • Senha SSH	• `install=(nfs,http,ftp,smb)://`*`caminho_mídia_inst`* • `usessh=1` • `sshpassword=`*`uma_senha`*
Seção 1.1.6, “Instalação remota por SSH: inicialização PXE e Wake on LAN” (p 29)	• Localização do servidor de instalação • Localização do servidor TFTP • Habilitação SSH • Senha SSH	Não aplicável; processo gerenciado via PXE e DHCP

DICA

Saiba mais sobre as opções de inicialização linuxrc usadas para inicializar um sistema Linux em `/usr/share/doc/packages/linuxrc/linuxrc.html`.

1.5 Monitorando o processo de instalação

Há várias opções para monitorar o processo de instalação remotamente. Se as opções de inicialização adequadas tiverem sido especificadas ao inicializar para instalação, VNC ou SSH podem ser usados para controlar a instalação e a configuração do sistema a partir de uma estação de trabalho remota.

1.5.1 Instalação VNC

Usando um software visualizador VNC, você pode controlar remotamente a instalação do SUSE Linux de virtualmente qualquer sistema operacional. Esta seção apresenta a configuração usando um visualizador VNC ou um browser da Web.

Preparando para instalação VNC

Tudo o que você precisa fazer no destino da instalação para preparar uma instalação VNC é fornecer as opções de inicialização adequadas na inicialização inicial para instalação (consulte a Seção 1.4.3, “Usando opções de inicialização personalizadas” (p 52)). O sistema de destino inicializa em um ambiente baseado em texto e espera que um cliente VNC conecte-se ao programa de instalação.

O programa de instalação anuncia o endereço IP e exibe o número necessário a conectar para instalação. Se você tiver acesso físico ao sistema de destino, essas informações são fornecidas logo depois do sistema ser inicializado para instalação. Digite esses dados quando eles forem solicitados pelo software cliente VNC e forneça a sua senha VNC.

Como o destino da instalação anuncia a si mesmo por OpenSLP, você pode recuperar a informação do endereço do destino da instalação com um browser SLP sem a

necessidade de qualquer contato físico com a instalação em si, desde que a sua configuração de rede e todas as máquinas tenham suporte a OpenSLP:

1. Inicie o arquivo KDE e o browser da Web Konqueror.

2. Digite `service://yast.installation.suse` na barra de localização.

   O sistema de destino aparece como um ícone na tela do Konqueror. Clicar neste ícone inicia o visualizador VNC do KDE no qual executar a instalação. Outra alternativa é executar o seu software visualizador VNC com o endereço IP fornecido e adicionar `:1` no final do endereço IP para exibir a instalação que está sendo executada.

Conectando-se ao programa de instalação

Basicamente, há duas maneiras de se conectar a um servidor VNC (o destino de instalação, neste caso). Você pode iniciar um visualizador VNC independente em qualquer sistema operacional ou conectar-se usando um browser da Web habilitado para Java.

Com o VNC, é possível controlar a instalação de um sistema Linux de qualquer outro sistema operacional, incluindo outras variedades do Linux, Windows ou Mac OS.

Em uma máquina Linux, verifique se o pacote `tightvnc` está instalado. Em uma máquina Windows, instale a porta Windows deste aplicativo, que pode ser obtida na home page do TightVNC (`http://www.tightvnc.com/download.html`).

Para conectar-se ao programa de instalação executado na máquina de destino, proceda da seguinte maneira:

1. Inicie o visualizador VNC.

2. Digite o endereço IP e o número de exibição do destino de instalação como fornecidos pelo browser SLP ou pelo próprio programa de instalação:

   endereço_ip:*número_exibição*

Uma janela é aberta na área de trabalho, mostrando as telas do YaST como em uma instalação local normal.

Ao usar um browser da Web para conectar-se ao programa de instalação, você fica totalmente independente de qualquer software VNC ou do sistema operacional subjacente. Visto que o aplicativo browser tenha o suporte Java habilitado, você pode usar qualquer browser (Firefox, Internet Explorer, Konqueror, Opera etc.) para executar a instalação do sistema Linux.

Para executar uma instalação VCN, proceda da seguinte maneira:

1. Inicie o seu browser da Web favorito.
2. Digite o seguinte no prompt de endereço:

   ```
   http://endereço_ip_do_destino:5801
   ```

3. Digite sua senha VNC quando solicitado. A janela do browser agora exibe as telas do YaST como em uma instalação local normal.

1.5.2 Instalação SSH

Com o SSH, você pode controlar remotamente a instalação da sua máquina Linux usando qualquer software cliente SSH.

Preparando para instalação SSH

Além de instalar o pacote de software adequado (OpenSSH para Linux e PuTTY para Windows), você só precisa passar as opções de inicialização adequadas para habilitar o SSH para instalação. Consulte a Seção 1.4.3, “Usando opções de inicialização personalizadas” (p 52) para obter detalhes. O OpenSSH é instalado por padrão em qualquer sistema operacional baseado no SUSE Linux.

Conectando-se ao programa de instalação

1. Recupere o endereço IP do destino da instalação.

Se você tiver acesso físico à máquina de destino, basta usar o endereço IP fornecido pelas rotinas de instalação no console após a primeira inicialização. Caso contrário, use o endereço IP que foi atribuído a este host específico na configuração de servidor DHCP.

2 Em uma linha de comando, digite o seguinte comando:

```
ssh -X root@endereço_ip_do_destino
```

Substitua *endereço_ip_do_destino* pelo endereço IP real do destino de instalação.

3 Quando for solicitado um nome de usuário, digite `root`.

4 Quando for solicitada uma senha, digite a senha que foi definida pela opção de inicialização do SSH.

Depois que você autenticar com êxito, será exibido um prompt de linha de comando para o destino da instalação.

5 Digite `yast` para iniciar o programa de instalação.

Uma janela é aberta mostrando as telas normais do YaST como descrito no Chapter *Instalação com o YaST* (↑Inicialização).

2 Configuração de disco avançada

As configurações sofisticadas do sistema requerem configurações de disco especiais. Para obter uma nomeação persistente em dispositivos SCSI, use um script de inicialização específico. O LVM (Logical Volume Management - Gerenciamento de Volumes Lógicos) é um esquema de particionamento de disco projetado para ser muito mais flexível que o particionamento físico usado nas configurações padrão. Sua funcionalidade de instantâneo permite criar facilmente backups de dados. A RAID (Redundant Array of Independent Disks - Matriz Redundante de Discos Independentes) oferece maior integridade de dados, desempenho e tolerância a falhas.

2.1 Nomes permanentes para dispositivos SCSI

Quando o sistema é inicializado, são designados nomes de arquivo aos dispositivos SCSI de uma forma mais ou menos dinâmica. Isso não representa um problema, desde que o número ou a configuração dos dispositivos não mude. No entanto, se um novo disco rígido SCSI for adicionado e detectado pelo kernel antes do disco rígido antigo, será designado um novo nome ao disco antigo, e a entrada na tabela de montagem `/etc/fstab` não corresponderá mais.

Para evitar esse problema, é possível usar o script de inicialização do sistema`boot.scsidev`. Habilite esse script usando `/sbin/insserv` e defina parâmetros para ele em `/etc/sysconfig/scsidev`. O script `/etc/rc.d/boot.scsidev` gerencia a configuração dos dispositivos SCSI durante o procedimento de inicialização e insere nomes de dispositivo permanentes em `/dev/scsi/`. Em seguida, esses nomes

podem ser usados em `/etc/fstab`. Além disso, o `/etc/scsi.alias` pode ser usado para definir nomes persistentes para a configuração SCSI. O esquema de nomeação dos dispositivos em `/etc/scsi` é explicado em `man scsidev`.

No modo de especialista do editor do runlevel, ative `boot.scsidev` para o nível `B`. Os links necessários para gerar os nomes durante o procedimento de inicialização são criados em `/etc/init.d/boot.d`.

DICA: Nomes de dispositivos e udev

No SUSE Linux, apesar de o `boot.scsidev` ainda ser suportado, a melhor forma de criar nomes de dispositivo persistentes é usar o udev para criar nós de dispositivo com nomes persistentes no `/dev/by-id/`.

2.2 Configuração da LVM

Esta seção descreve brevemente os princípios por trás do LVM e os recursos básicos que o tornam úteis em várias circunstâncias. Na Seção 2.2.2, “Configuração do LVM com o YaST” (p 62), aprenda como configurar o LVM com o YaST.

ATENÇÃO

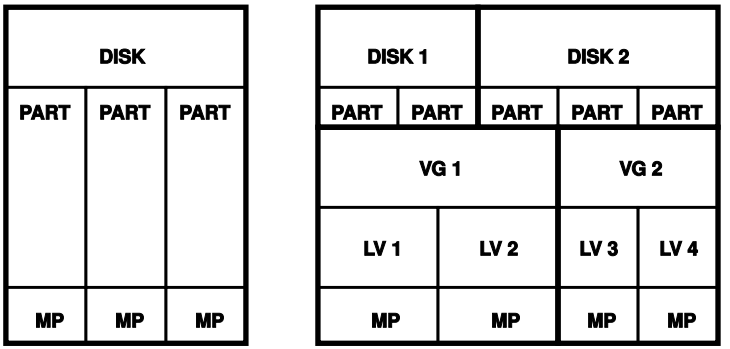
A utilização do LVM pode se associada a um aumento de risco, como perda de dados. O risco também inclui falhas de aplicativo, de energia e em comandos. Grave os dados antes de implementar o LVM ou reconfigurar volumes. Nunca trabalhe sem backup.

2.2.1 Gerenciador de Volumes Lógicos

O LVM (Logical Volume Manager - Gerenciador de Volumes Lógicos) permite uma distribuição flexível de espaço em disco rígido em vários sistemas de arquivos. Ele foi desenvolvido porque algumas vezes a necessidade de mudar a segmentação do espaço no disco rígido surge apenas depois que é feito o particionamento inicial durante a instalação. Como é difícil modificar partições em um sistema em execução, o LVM fornece um pool virtual, ou seja, VG (Volume Group - Grupo de Volume) de espaço em memória com base no qual os LVs (Logical Volumes - Volumes Lógicos) podem ser criados conforme o necessário. O sistema operacional acessa esses LVs, em vez de

acessar as partições físicas. Os grupos de volume podem ocupar mais de um disco; portanto, vários discos ou partes deles podem constituir um único VG. Dessa forma, o LVM fornece um tipo de abstração a partir do espaço do disco físico que permite que sua segmentação seja mudada de uma forma mais fácil e segura do que o reparticionamento físico proporciona. É possível encontrar outras informações sobre o particionamento físico na “Tipos de partição” (Capítulo 1, *Instalação com o YaST*, ↑Inicialização) e naSeção “Particionador” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

Figura 2.1 *Particionamento físico versus LVM*



A Figura 2.1, “Particionamento físico versus LVM” (p 61) compara o particionamento físico (esquerda) com a segmentação do LVM (direita). Do lado esquerdo, um único disco rígido foi dividido em três PART (Physical Partitions - Partições Físicas), cada uma com um MP (Mount Point - Ponto de Montagem) designado, de forma que o sistema operacional possa acessá-las. Do lado direito, dois discos foram divididos em duas e três partições físicas cada. Foram definidos dois grupos de volume (VG1 e VG2) do LVM. O VG1 contém duas partições do DISCO 1 e uma do DISCO 2. O VG2 contém as duas partições restantes do DISCO 2. No LVM, as partições físicas do disco incorporadas a um grupo de volume são chamadas de PVs (physical volumes - volumes físicos). Nos grupos de volume, foram definidos quatro volumes lógicos (LV1 a LV4), que podem ser usados pelo sistema operacional por meio dos pontos de montagem associados. A fronteira entre os volumes lógicos diferentes não deve ser alinhada com as fronteiras das partições. Veja a fronteira entre LV1 e LV2 neste exemplo.

Recursos do LVM:

- vários discos rígidos ou partições podem ser combinados em um grande volume lógico.

- Desde que a configuração seja adequada, um LV (como `/usr`) pode ser ampliado quando o espaço em disco estiver esgotado.

- Usando o LVM, adicione discos rígidos ou LVs em um sistema em execução. No entanto, esse procedimento requer um hardware altamente permutável, capaz de executar tais ações.

- É possível ativar um "modo de distribuição" que distribui o fluxo de dados de um volume lógico em vários volumes físicos. Se esses volumes físicos residirem em discos diferentes, o desempenho de leitura e gravação poderá ser melhorado como ocorre com o RAID 0.

- O recurso instantâneo permite backups consistentes (especialmente para servidores) no sistema em execução.

Com esses recursos, a utilização do LVM é sensata em PCs domésticos muito usados ou pequenos servidores. Se você tem um estoque de dados crescente, como no caso de bancos de dados, arquivos de música ou diretórios de usuário, o LVM é simplesmente a opção correta. Ele permite o uso de sistemas de arquivos maiores do que o disco rígido físico. Outra vantagem do LVM é a possibilidade de adicionar até 256 LVs. Entretanto, lembre-se de que trabalhar com o LVM é diferente de trabalhar com partições convencionais. Instruções e informações adicionais sobre a configuração do LVM estão disponíveis no HOWTO (Como Fazer) oficial do LVM, em `http://tldp.org/HOWTO/LVM-HOWTO/`.

Começando na versão 2.6 do kernel, a versão 2 do LVM está disponível, sendo compatível com versões anteriores do LVM e permitindo o gerenciamento contínuo de antigos grupos de volume. Ao criar novos grupos de volume, decida se vai usar o novo formato ou a versão compatível com versões anteriores. O LVM 2 não requer qualquer patch de kernel. Ele usa o mapeador de dispositivos integrado ao kernel 2.6. Esse kernel suporta somente a versão 2 do LVM. Portanto, sempre que o LVM for abordado nesta seção, será considerada a versão 2.

2.2.2 Configuração do LVM com o YaST

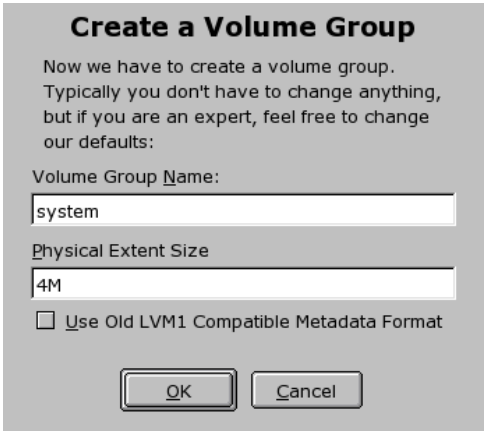
A configuração do LVM com YaST pode ser feita com o Particionador Expert do YaST (consulte aSeção “Particionador” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização)). Essa ferramenta profissional de particionamento permite editar e apagar partições existentes, e criar novas que devem ser usadas com o LVM. Crie uma partição

do LVM clicando primeiro em *Criar → Não formatar* e selecionando *0x8E Linux LVM* como identificador de partição. Depois de criar todas as partições para usar o LVM, clique em *LVM* para iniciar sua configuração.

Criando grupos de volume

Se ainda não houver grupos de volume no sistema, você será solicitado a adicionar um (consulte aFigura 2.2, “Criando um grupo de volume” (p 63)). É possível criar grupos adicionais com a opção *Adicionar*, mas normalmente um único grupo de volume é suficiente. O nome sugerido para o grupo de volume em que os arquivos do sistema SUSE Linux se localizarão é `system`. O tamanho físico de extensão define o tamanho de um bloco físico no grupo de volume. Todo o espaço em disco de um grupo de volume é gerenciado em pacotes desse tamanho. Esse valor é normalmente definido como 4 MB e permite um tamanho máximo de 256 GB para volumes físicos e lógicos. O tamanho físico de extensão só deve ser aumentado, por exemplo, para 8, 16 ou 32 MB, se você precisar de volumes lógicos maiores que 256 GB.

Figura 2.2 *Criando um grupo de volume*



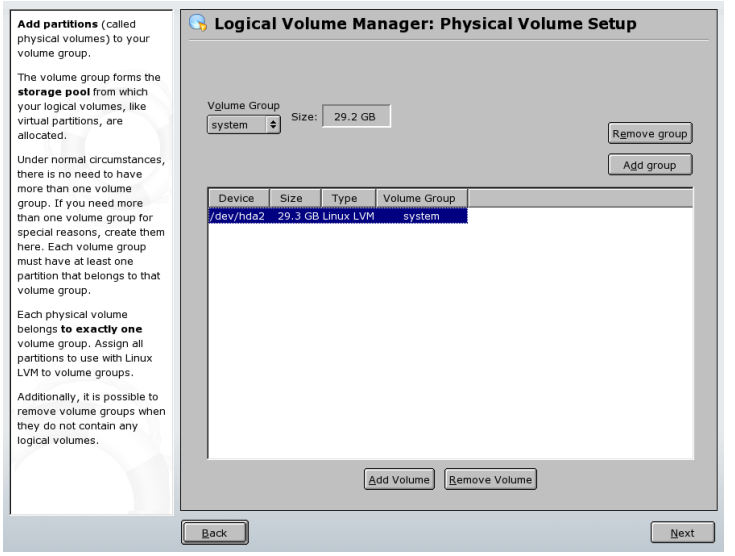
Configurando volumes físicos

Depois que um grupo de volume é criado, a caixa de diálogo a seguir lista todas as partições com os tipos “LVM do Linux” ou “nativas do Linux”. Nenhuma partição DOS ou de troca é mostrada. Se uma partição já tiver sido designada a um grupo de

volume, o nome dele será exibido na lista. Partições não designadas são indicadas com "--".

Se houver vários grupos de volume, defina o grupo de volume atual na caixa de seleção do canto superior esquerdo. Os botões do canto superior direito permitem criar grupos de volume adicionais, bem como apagar grupos de volumes existentes. Somente grupos de volume sem partições designadas podem ser apagados. Todas as partições designadas a um grupo de volume também são citadas como um PV (Physical Volume - Volume Físico).

Figura 2.3 *Configuração do volume físico*

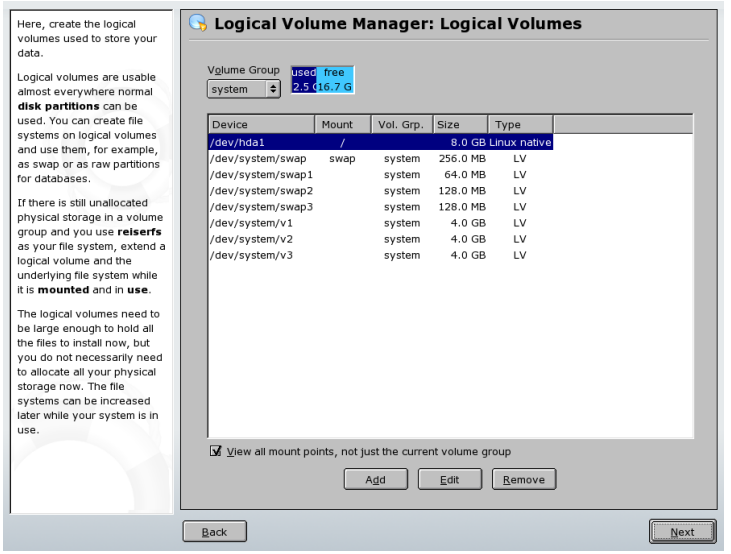

Add partitions (called physical volumes) to your volume group.
The volume group forms the storage pool from which your logical volumes, like virtual partitions, are allocated.
Under normal circumstances, there is no need to have more than one volume group. If you need more than one volume group for special reasons, create them here. Each volume group must have at least one partition that belongs to that volume group.
Each physical volume belongs to exactly one volume group. Assign all partitions to use with Linux LVM to volume groups.
Additionally, it is possible to remove volume groups when they do not contain any logical volumes.
Logical Volume Manager: Physical Volume Setup
Volume Group
system
Size:
29.2 GB
Remove group
Add group
Device
Size
Type
Volume Group
/dev/hda2
29.3 GB Linux LVM
system
Add Volume
Remove Volume
Back
Next

Para adicionar uma partição previamente não designada ao grupo de volume selecionado, primeiro clique na partição, depois clique em *Adicionar Volume*. Nesse momento, o nome do grupo de volume é inserido ao lado da partição selecionada. Designe todas as partições reservadas para o LVM a um grupo de volume. Caso contrário, o espaço da partição permanecerá não utilizado. Antes de sair da caixa de diálogo, é necessário designar pelo menos um volume físico a cada grupo de volume. Depois de designar todos os volumes físicos, clique em *Próximo* para continuar a configuração de volumes lógicos.

Configurando volumes lógicos

Depois de o grupo de volume ser preenchido com volumes físicos, defina os volumes lógicos que o sistema operacional deverá usar na próxima caixa de diálogo. Defina o grupo de volume atual em uma caixa de seleção no canto superior esquerdo. Ao lado dela, é exibido o espaço livre no grupo de volumes atual. A lista a seguir contém todos os volumes lógicos do grupo de volume. Todas as partições normais do Linux às quais um ponto de montagem é designado, todas as partições de troca e todos os volumes lógicos já existentes são listados aqui. *Adicione*, *edite* e *remova* volumes lógicos conforme o necessário, até esgotar todo o espaço do grupo de volume. Designe pelo menos um volume lógico a cada grupo de volume.

Figura 2.4 *Gerenciamento de volume lógico*


Here, create the logical volumes used to store your data.
Logical volumes are usable almost everywhere normal disk partitions can be used. You can create file systems on logical volumes and use them, for example, as swap or as raw partitions for databases.
If there is still unallocated physical storage in a volume group and you use reiserfs as your file system, extend a logical volume and the underlying file system while it is mounted and in use.
The logical volumes need to be large enough to hold all the files to install now, but you do not necessarily need to allocate all your physical storage now. The file systems can be increased later while your system is in use.
Logical Volume Manager: Logical Volumes
Volume Group
system
used free
2.5 G 16.7 G
Device Mount Vol. Grp. Size Type
/dev/hda1 / 8.0 GB Linux native
/dev/system/swap swap system 256.0 MB LV
/dev/system/swap1 system 64.0 MB LV
/dev/system/swap2 system 128.0 MB LV
/dev/system/swap3 system 128.0 MB LV
/dev/system/v1 system 4.0 GB LV
/dev/system/v2 system 4.0 GB LV
/dev/system/v3 system 4.0 GB LV
View all mount points, not just the current volume group
Add
Edit
Remove
Back
Next

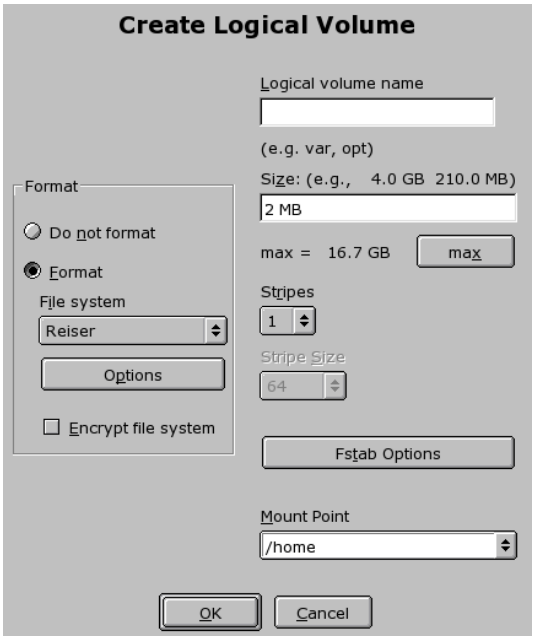
Para criar um novo volume lógico, clique em *Adicionar* e preencha a janela que é aberta. No que diz respeito ao particionamento, digite o tamanho, o sistema de arquivos e o ponto de montagem. Normalmente, um sistema de arquivos, como reiserfs ou ext2, é criado em um volume lógico e então um ponto de montagem é designado a ele. Os arquivos armazenados nesse volume lógico podem ser encontrados nesse ponto de montagem do sistema instalado. Além disso, é possível distribuir o fluxo de dados no volume lógico entre vários volumes físicos. Se esses volumes físicos residirem em discos rígidos diferentes, os desempenhos de leitura e gravação podem ser melhorados

(como ocorre com RAID 0). No entanto, um LV de distribuição com `n` distribuições só poderá ser criado corretamente se o espaço em disco rígido necessário para o LV puder ser distribuído uniformemente em `n` volumes físicos. Se, por exemplo, houver apenas dois volumes físicos disponíveis, será impossível haver um volume lógico com três distribuições.

ATENÇÃO: Distribuindo

A essa altura, o YaST não tem como verificar se suas entradas estão corretas no que diz respeito à distribuição. Qualquer erro realizado aqui será mostrado somente mais tarde, quando o LVM for implementado em disco.

Figura 2.5 *Criando volumes lógicos*



Se você já configurou o LVM no sistema, os volumes lógicos existentes poderão ser inseridos agora. Antes de continuar, designe pontos de montagem apropriados a esses volumes lógicos também. Usando a opção *Próximo*, volte para o Particionador Expert do YaST e conclua seu trabalho.

Gerenciamento direto do LVM

Se você já configurou o LVM e só quer mudar alguma coisa, há uma forma alternativa de fazê-lo. No Centro de Controle do YaST, selecione *Sistema → LVM*. Essa caixa de diálogo basicamente permite as mesmas ações descritas anteriormente, com a exceção do particionamento físico. Ela mostra os volumes físicos e os volumes lógicos existentes em duas listas, e você pode gerenciar seu sistema LVM usando os métodos já descritos.

2.3 Configuração de RAID de software

A finalidade do RAID (redundant array of inexpensive disks) é combinar várias partições de disco rígido em um grande disco rígido *virtual* para otimizar o desempenho, a segurança dos dados ou ambos. Quando esse método é usado, no entanto, uma vantagem é obtida em detrimento de outra. A maioria das controladoras RAID usa o protocolo SCSI porque ele é capaz de lidar com um grande número de discos rígidos com mais eficiência que o protocolo IDE, além de ser mais apropriado para o processamento de comandos em paralelo. Algumas controladoras RAID suportam discos rígidos IDE ou SATA. Consulte o site de banco de dados de hardware em `http://cdb.suse.de`.

2.3.1 RAID de software

O RAID de software é capaz de executar as mesmas tarefas que uma controladora RAID, que pode ser bastante cara. O SUSE Linux oferece a opção de combinar vários discos rígidos em um sistema RAID de software com a ajuda do YaST, uma alternativa bastante razoável ao RAID de hardware. O RAID requer diversas estratégias para a combinação de vários discos rígidos em um sistema RAID, cada uma delas com diferentes objetivos, vantagens e características. Essas variações geralmente são conhecidas como *níveis de RAID*.

Os níveis de RAID comuns são:

RAID 0
: Esse nível melhora o desempenho do acesso aos dados dividindo blocos de cada arquivo entre várias unidades de disco. Na verdade, isso não é realmente um RAID, porque não oferece o backup dos dados, mas o nome *RAID 0* para esse tipo de

sistema tornou-se uma norma. Com o RAID 0, dois ou mais discos rígidos são unidos em um pool. O desempenho é muito bom, mas, em caso de falha até mesmo de um disco rígido, o sistema RAID é destruído e seus dados são perdidos.

RAID 1

Esse nível fornece a segurança adequada para seus dados, porque eles são copiados para outro disco rígido 1:1. Isso é conhecido como *espelhamento de disco rígido*. Se um disco for destruído, uma cópia de seu conteúdo estará disponível em outro disco. Mesmo que todos os discos, com exceção de um, sejam danificados, você não corre o risco de perder seus dados. O desempenho de gravação fica um pouco prejudicado no processo de cópia, em comparação ao uso do acesso a um único disco (dez a vinte por cento mais lento), mas o acesso de leitura é significativamente mais rápido se comparado com o de qualquer um dos discos rígidos físicos normais, uma vez que os dados são duplicados e, conseqüentemente, podem ser explorados em paralelo. Em geral, pode-se dizer que o Nível 1 fornece praticamente o dobro da velocidade de transação de leitura dos discos individuais e quase a mesma velocidade de transação de gravação que eles.

RAID 2 e RAID 3

Essas são implementações de RAID não muito comuns. O Nível 2 divide os dados no nível de bits, em vez de no nível de blocos. O Nível 3 fornece a divisão no nível de bytes com um disco de paridade dedicada, e não pode atender várias solicitações ao mesmo tempo. Ambos os níveis raramente são usados.

RAID 4

O Nível 4 fornece a divisão no nível de blocos, exatamente como o Nível 0 combinado com um disco de paridade dedicada. No caso de uma falha de disco de dados, os dados de paridade são usados para criar um disco de substituição. No entanto, o disco de paridade pode criar um gargalo para o acesso de gravação. Mesmo assim, o Nível 4 às vezes é usado.

RAID 5

O RAID 5 é um compromisso otimizado entre o Nível 0 e o Nível 1 em termos de desempenho e redundância. O espaço em disco rígido é igual ao número de discos usados menos um. Os dados são distribuídos pelos discos rígidos, assim como no RAID 0. Os *blocos de paridade*, criados em uma das partições, estão lá por motivos de segurança. Eles são vinculados uns aos outros com XOR, o que habilita o conteúdo, via XOR, para ser reconstruído pelo bloco de paridade correspondente no caso de uma falha do sistema. Com o RAID 5, apenas um disco rígido pode

falhar por vez. Se um disco rígido falhar, ele deverá ser substituído assim que possível, para evitar o risco da perda de dados.

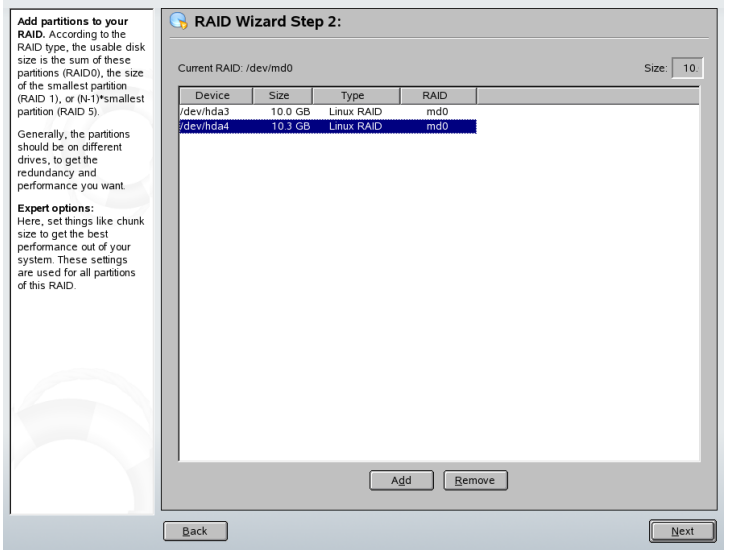
Outros níveis de RAID
Vários outros níveis de RAID foram desenvolvidos (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.), sendo alguns deles implementações proprietárias criadas por fornecedores de hardware. Esses níveis não estão muitos difundidos, portanto, não serão explicados aqui.

2.3.2 Configuração de RAID de software com o YaST

A configuração de RAID de software do YaST pode ser obtida a partir do Particionador Expert do YaST, descrito na Seção “Particionador” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização). Essa ferramenta profissional de particionamento permite editar e excluir partições existentes e criar novas partições que devem ser usadas com o RAID de software. Nela, você cria partições RAID clicando em *Criar* → *Não formatar* e, em seguida, selecionando *0xFD Linux RAID* como identificador de partição. Para o RAID 0 e o RAID 1, pelo menos duas partições são necessárias; para o RAID 1, geralmente são necessárias exatamente duas partições, não mais. Se o RAID 5 for usado, pelo menos três partições serão necessárias. É recomendável usar apenas partições com o mesmo tamanho. As partições RAID devem ser armazenadas em diferentes discos rígidos para diminuir o risco da perda de dados caso um deles esteja danificado (RAID 1 e 5) e para otimizar o desempenho do RAID 0. Após criar todas as partições para uso com o RAID, clique em *RAID* → *Criar RAID* para iniciar a configuração do RAID.

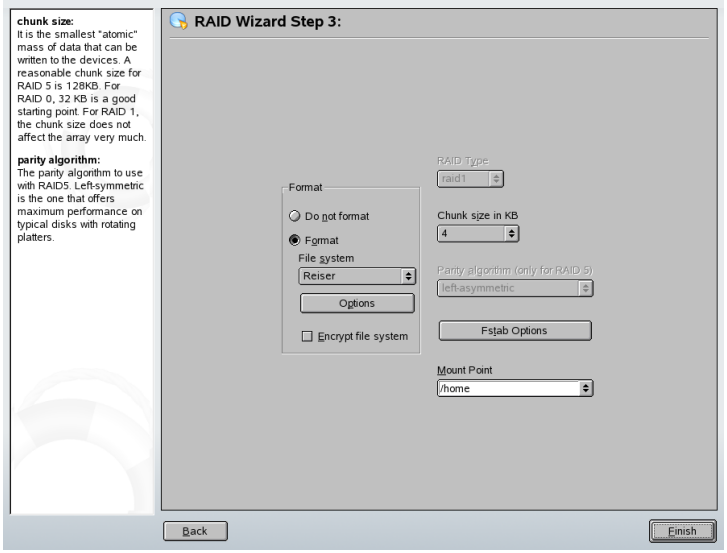
Na caixa de diálogo seguinte, escolha entre os níveis de RAID 0, 1 e 5 (consulte a Seção 2.3.1, “RAID de software” (p 67) para obter detalhes). Após clicar em *Próximo*, a caixa de diálogo a seguir lista todas as partições com o tipo “RAID Linux” ou “nativo do Linux” (consulte a Figura 2.6, “Partições RAID” (p 70)). Não são exibidas partições do DOS ou de troca. Se uma partição já estiver atribuída a um volume RAID, o nome do dispositivo de RAID (por exemplo, `/dev/md0`) será exibido na lista. As partições não atribuídas são indicadas com “--”.

Figura 2.6 *Partições RAID*


Add partitions to your RAID. According to the RAID type, the usable disk size is the sum of these partitions (RAID0), the size of the smallest partition (RAID 1), or (N-1)*smallest partition (RAID 5).
Generally, the partitions should be on different drives, to get the redundancy and performance you want.
Expert options:
Here, set things like chunk size to get the best performance out of your system. These settings are used for all partitions of this RAID.
RAID Wizard Step 2:
Current RAID: /dev/md0
Size:
10
Device
Size
Type
RAID
/dev/hda3
10.0 GB
Linux RAID
md0
/dev/hda4
10.3 GB
Linux RAID
md0
Add
Remove
Back
Next

Para adicionar uma partição anteriormente não atribuída ao volume RAID selecionado, primeiro clique na partição e, em seguida, em *Adicionar*. Nesse ponto, o nome do dispositivo de RAID é inserido ao lado da partição selecionada. Atribua todas as partições reservadas para o RAID. Caso contrário, o espaço na partição permanecerá sem uso. Após atribuir todas as partições, clique em *Próximo* para continuar na caixa de diálogo de configurações, onde você pode ajustar o desempenho (consulte a Figura 2.7, “Configurações do sistema de arquivos” (p 71)).

Figura 2.7 *Configurações do sistema de arquivos*


chunk size:
It is the smallest "atomic" mass of data that can be written to the devices. A reasonable chunk size for RAID 5 is 128KB. For RAID 0, 32 KB is a good starting point. For RAID 1, the chunk size does not affect the array very much.
parity algorithm:
The parity algorithm to use with RAID5. Left-symmetric is the one that offers maximum performance on typical disks with rotating platters.
RAID Wizard Step 3:
RAID Type
raid1
Format
Do not format
Format
File system
Reiser
Options
Encrypt file system
Chunk size in KB
4
Parity algorithm (only for RAID 5)
left-asymmetric
Fstab Options
Mount Point
/home
Back
Finish

Assim como no particionamento convencional, defina o sistema de arquivos a ser usado, assim como a criptografia e o ponto de montagem do volume RAID. Marcar *Superbloco Persistente* garante que as partições RAID sejam reconhecidas como tais na inicialização. Após concluir a configuração com *Concluir*, verifique o dispositivo `/dev/md0` e outros dispositivos indicados com *RAID* no particionador expert.

2.3.3 Solução de problemas

Verifique o arquivo `/proc/mdstats` para saber se uma partição RAID foi destruída. No caso de uma falha do sistema, encerre o sistema Linux e substitua o disco rígido danificado por um novo, particionado da mesma maneira. Depois, reinicie o sistema e digite o comando `mdadm /dev/mdX --add /dev/sdX`. Substitua 'X' por seus próprios identificadores de dispositivo. Isso integra o disco rígido automaticamente ao sistema RAID e o reconstrói totalmente.

2.3.4 Para obter mais informações

Instruções de configuração e mais detalhes sobre o RAID de software podem ser encontrados nos HOWTOs, em:

- `/usr/share/doc/packages/raidtools/Software-RAID.HOWTO.html`
- http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html

Também estão disponíveis listas de discussão relacionadas ao RAID do Linux, como em http://www.mail-archive.com/linux-raid@vger.rutgers.edu.

Parte II Internet

3 Browser da Web Konqueror

O Konqueror não é apenas um gerenciador de arquivos versátil, é também um moderno browser da Web. Quando você inicia o browser usando o ícone no painel, o Konqueror é aberto com o perfil do browser da Web. Como browser, o Konqueror oferece navegação por meio de guias, a possibilidade de salvar páginas da Web com gráficos, palavras-chave da Internet e suporte para Java e JavaScript.

Inicie o Konqueror a partir do menu principal ou inserindo o comando `konqueror`. Para carregar uma página da Web, insira o seu endereço na barra de local, por exemplo, `http://www.suse.com`. O Konqueror agora tenta alcançar o endereço e exibir a página. Inserir o protocolo no início do endereço (`http://` neste caso) não é estritamente necessário. O programa também é capaz de completar o endereço automaticamente, mas isso só funciona de forma confiável com endereços da Web. Para um endereço de FTP, sempre insira `ftp://` no início do campo de entrada.

Figura 3.1 *Janela do browser do Konqueror*

Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://konqueror.kde.org/
Konqueror Homepage
Location: Konqueror Homepage
Sitemap :: Help :: Contact Us
Inform
Home
KDE Home
Announcements
News
Features
Konqueror Embedded
Technical
Konqueror FAQ
Java HOWTO
CSS Support
Download
Konqueror - Web Browser, File Manager - and more!
Konqueror is the file manager for the K Desktop Environment. It supports basic file management on local UNIX filesystems, from simple cut/copy and paste operations to advanced remote and local network file browsing.
Konqueror is the canvas for all the latest KDE technology, from KIO slaves (which provide mechanisms for file access) to component embedding via the KParts object interface, and it is one of the most customizable applications
Search
kde.org
Search
KDE Family
» News & Information
KDE News
KDE Events
KDE Myths
» KDE Projects

3.1 Navegação em guias

Se você normalmente usa mais de uma página da Web de uma só vez, a navegação em guias pode facilitar a alternância entre elas. Carregue sites na Web em guias separadas em uma única janela. A vantagem é que você mantém controle sobre sua área de trabalho pois só tem uma janela principal. Após o logout, o gerenciamento de sessão do KDE permite salvar sua sessão da Web no Konqueror. Na próxima vez em que você efetuar login, o Konqueror carrega os URLs exatos visitados na última vez.

Para abrir uma nova guia, selecione *Janela* → *Nova Guia* ou pressione Ctrl + Shift + N. Para alterar o comportamento das guias, vá para *Configurações* → *Configurar Konqueror*. Na caixa de diálogo aberta, selecione *Comportamento Web* → *Navegação em Guias*. Para abrir novas guias em vez de janelas, habilite *Abrir links em uma nova guia ao invés de em uma nova janela*. Você também pode ocultar a barra de guias com *Ocultar a barra de guias quando somente uma guia estiver aberta*. Para ver mais opções, pressione *Opções Avançadas*.

Você pode salvar suas guias com URLs e a posição de uma janela em um perfil. Isso é um pouco diferente do gerenciamento de sessão mencionado acima. Com perfis, você tem suas guias salvas e acessíveis e sem o tempo de inicialização intensivo como com o gerenciamento de sessão.

No Konqueror, vá para *Configurações → Configurar Perfis de Visão* e forneça um nome a seu perfil. Você pode salvar o tamanho da janela no perfil também com a respectiva opção. Verifique se *Salvar URLs no perfil* está selecionado. Aprove com *Salvar*. Na próxima vez que você precisar da "coleção de guias," vá para *Configurar → Carregar Perfil de Visão* e veja o nome listado no menu. Após selecionar o nome, o Konqueror restaura suas guias.

3.2 Gravando páginas da Web e elementos gráficos

Como em outros navegadores, é possível gravar páginas da Web. Para fazer isso, selecione *Localização → Salvar como* e especifique um nome para o arquivo HTML. No entanto, as imagens não serão gravadas. Para arquivar uma página da Web inteira, inclusive as imagens, selecione *Ferramentas → Arquivar página web*. O Konqueror sugere um nome de arquivo que você pode em geral aceitar. O nome de arquivo termina com `.war`, a extensão usada para arquivos Web. Para ver o arquivo gravado, basta clicar no arquivo correspondente e a página da Web será exibida no Konqueror com as imagens.

3.3 Palavras-chave da Internet

Efetuar pesquisas na Web usando o Konqueror é uma tarefa muito fácil. O Konqueror define mais de 70 filtros de busca para você, todos com um atalho específico. Para pesquisar determinado tópico na Internet, digite o atalho e a palavra-chave separados por dois-pontos. A página relevante com os resultados da pesquisa é exibida.

Para ver os atalhos já definidos, vá para *Configurações → Configurar Konqueror*. Na caixa de diálogo que aparece, selecione *Atalhos da Web*. Agora você pode ver os nomes dos provedores de busca e os atalhos. O Konqueror define vários filtros de busca: os mecanismos de busca "clássicos", como Google, Yahoo e Lycos e vários filtros para

propósitos menos comuns, como um banco de dados de acrônimos, o banco de dados de filmes da Internet ou buscas de aplicativos de KDE.

Se você não encontrar o seu mecanismo de busca preferido aqui, defina um facilmente. Por exemplo, para pesquisar nosso banco de dados de suporte em busca de alguns artigos interessantes, normalmente vá para `http://portal.suse.com/`, localize a página de busca e insira sua consulta. Isso pode ser simplificado usando atalhos. Na caixa de diálogo mencionada, selecione *Novo* e forneça um nome ao atalho em *Procurar nome de provedor*. Insira suas abreviações em *Atalhos URI*. Pode haver mais de um, separado por vírgulas. O campo de texto importante é *URI de Busca*. Pressionar Shift + F1 e clicar no campo abre uma ajuda pequena. A consulta de busca é especificada como `\{@}`. O desafio é inserir isso na posição correta. Neste caso, as configurações para o banco de dados de suporte do SUSE têm a seguinte aparência: *Procurar nome de provedor* é `Banco de Dados de Suporte do SUSE`, *URI de Busca* é (uma linha) `https://portal.suse.com/PM/page/search.pm?q=\{@}&t=optionSdbKeywords&m=25&l=en&x=true` e *Atalhos URI* é `sdb_en`.

Após aprovar com *Ok* duas vezes, insira sua consulta na barra de local do Konqueror, por exemplo, `sdb_en:kernel`. O resultado é exibido na janela atual.

3.4 Favoritos

Em vez de lembrar e reinserir endereços para sites visitados com freqüência, você pode marcar esses URLs usando o menu *Favorito*. Além dos endereços de páginas da Web, também é possível marcar quaisquer diretórios do disco local desta forma.

Para criar um novo favorito no Konqueror, clique em *Favoritos → Adicionar Favorito*. Quaisquer marcadores adicionados previamente são incluídos como itens no menu. É uma boa idéia organizar a coleção de marcadores por assuntos em uma estrutura hierárquica, para que você não perca itens diferentes. Crie um novo subgrupo para seus favoritos com *Nova Pasta de Favoritos*. Selecionar *Favoritos → Editar Favoritos* abre o editor de favoritos. Use esse programa para organizar, reordenar, adicionar e apagar favoritos.

Se você estiver usando o Netscape, Mozilla ou o Firefox como browsers adicionais, não é necessário recriar seus favoritos. As opções *Arquivo → Importar Favoritos do Netscape*, no editor de favoritos, permitem integrar os favoritos do Netscape e do Mozilla à sua coleção mais atual. O inverso também é possível por meio de *Exportar como Favorito do Netscape* .

Mude seus favoritos clicando o botão direito do mouse sobre a entrada. No menu pop-up exibido, selecione a ação desejada (recortar, copiar, excluir etc). Quando estiver satisfeito com o resultado, salve os favoritos com *Arquivo → Salvar*. Se você deseja alterar somente o nome ou o link, clique o botão direito na entrada na barra de ferramenta de favoritos e selecione *Propriedades*. Altere o nome e o local e confirme com *Atualizar*.

Para gravar a lista de favoritos e ter acesso instantâneo a ela, torne os favoritos visíveis no Konqueror. Selecione *Configurações → Barra de Ferramentas → Barra de Ferramentas de Favoritos (Konqueror)*. Um painel de favoritos é automaticamente exibido na janela atual do Konqueror.

3.5 Java e JavaScript

Não confunda essas duas linguagens. Java é uma linguagem de programação da Sun Microsystems orientada ao objeto e que independe de plataforma. Ela é freqüentemente usada para pequenos programas (applets) executados na Internet para operações bancárias online, bate-papo e compras. JavaScript é uma linguagem de script, usada principalmente para a estruturação dinâmica de páginas da Web, por exemplo, para menus e outros efeitos.

O Konqueror permite habilitar ou desabilitar essas duas linguagens. Isso pode ser feito até mesmo de uma forma específica ao domínio, o que significa que você pode permitir acesso a alguns hosts e bloqueá-lo a outros. As linguagens Java e JavaScript são freqüentemente desabilitadas por questões de segurança. Infelizmente, algumas páginas da Web necessitam de JavaScript para serem visualizadas corretamente.

3.6 Para obter mais informações

Se você tiver quaisquer questões ou problemas ao trabalhar com o Konqueror, consulte o manual do aplicativo, que está disponível no menu *Ajuda*. O Konqueror também tem uma página da Web, localizada em `http://www.konqueror.org`.

4 Firefox

O SUSE Linux está incluído no browser da Web Mozilla Firefox. Com recursos como guias, bloqueio de janelas pop-up, download e gerenciamento de imagens, o Firefox combina as tecnologias da Web mais recentes. Exiba mais de uma página da Web em uma única janela. Suprima anúncios irritantes e desabilite imagens que só servem para reduzir sua produtividade. Seu fácil acesso a diversos mecanismos de pesquisa ajuda-o a encontrar as informações necessárias. Inicie o programa no menu principal ou digitando o comando `firefox`. Os principais recursos do programa serão descritos nas seções seguintes.

4.1 Navegando em sites na Web

O Firefox tem praticamente a mesma aparência e operacionalidade de outros browsers. Você pode ver isso na Figura 4.1, “Janela do browser do Firefox” (p 82). A barra de ferramentas de navegação contém ícones para *avançar* e *voltar* e uma barra de localização para endereços da Web. Também há marcadores disponíveis para garantir acesso rápido. Para obter mais informações sobre os vários recursos do Firefox, use o menu *Help* (Ajuda).

Figura 4.1 *Janela do browser do Firefox*

4.1.1 Navegação em guias

Se você normalmente usa mais de uma página da Web de uma só vez, a navegação em guias pode facilitar a alternância entre elas. Carregue sites na Web em guias separadas em uma única janela.

Para abrir uma nova guia, selecione *File → New Tab* (Arquivo - Nova Guia). Esse procedimento abre uma guia vazia na janela do Firefox. Como alternativa, clique o botão direito do mouse em um link e selecione *Open link in new tab* (Abrir link em nova guia). Clique o botão direito na guia para acessar mais opções. Você pode criar uma nova guia, recarregar uma ou todas elas ou fechá-las.

4.1.2 Usando a barra lateral

Use o lado esquerdo da janela do browser para exibir os marcadores ou o histórico de navegação. As extensões também podem permitir novas maneiras de usar a barra lateral. Para exibir a barra lateral, selecione *View → Sidebar (Exibir - Barra Lateral)* e selecione o conteúdo desejado.

4.2 Localizando informações

Há duas maneiras de localizar informações no Firefox: a barra de pesquisa e a barra de localização. A barra de pesquisa procura páginas, ao passo que a barra de localização procura itens na página atual.

4.2.1 Usando a barra de pesquisa

O Firefox tem uma barra de pesquisa que pode acessar diversos mecanismos, como Google, Yahoo ou Amazon. Por exemplo, para localizar informações sobre o SUSE usando o mecanismo atual, clique na barra de pesquisa, digite `SUSE` e pressione Enter. Os resultados são exibidos na janela. Para escolher o mecanismo de pesquisa, clique no ícone na barra de pesquisa. É aberto um menu com uma lista de mecanismos de pesquisa disponíveis.

4.2.2 Usando a barra de localização

Para pesquisar em uma página da Web, clique em *Edit → Find in This Page* (Editar - Localizar Nesta Página) ou pressione Ctrl + F para abrir a barra de localização. Em geral, ela é exibida na parte inferior da janela. Digite sua consulta no campo de entrada. O Firefox realça todas as ocorrências dessa frase. Com *Highlight* (Realçar), habilite e desabilite o realce.

4.3 Gerenciando marcadores

Os marcadores oferecem uma maneira fácil de gravar links nos seus sites favoritos. Para adicionar o site na Web atual à lista de marcadores, clique em *Bookmarks →*

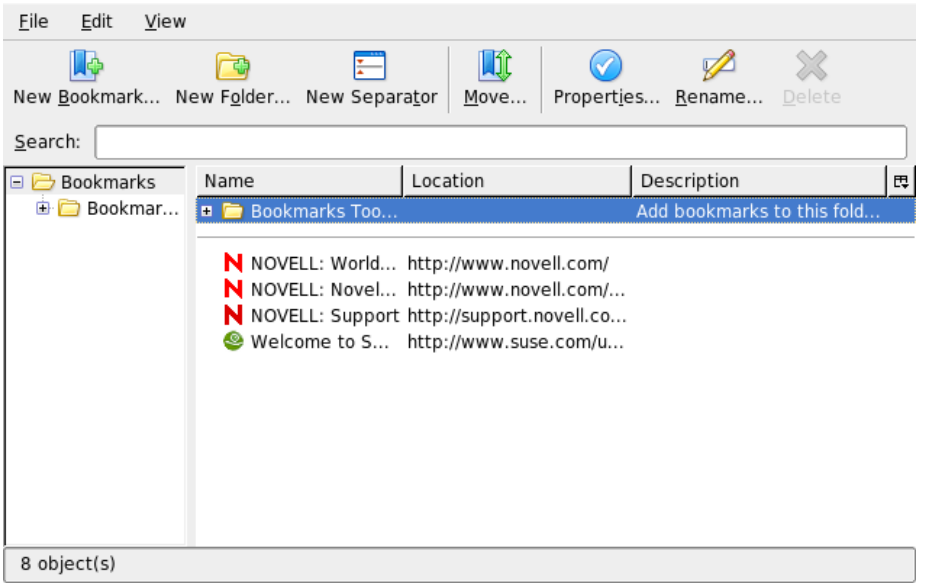
Bookmark This Page (Marcadores - Marcar Esta Página). Se o browser exibir vários sites da Web em guias, somente o URL da guia selecionada atualmente será adicionado à lista de marcadores.

Ao adicionar um marcador, você pode especificar outro nome para ele e selecionar uma pasta para o Firefox armazená-lo. Para remover um site da lista de marcadores, clique em *Bookmarks* (Marcadores), clique o botão direito do mouse no marcador e clique em *Delete* (Excluir).

4.3.1 Usando o gerenciador de marcadores

O gerenciador de marcadores pode ser usado para gerenciar as propriedades (nome e endereço) de cada marcador, como também organizar os marcadores em pastas e seções. Ele se assemelha à Figura 4.2, “Usando o gerenciador de marcadores do Firefox” (p 84).

Figura 4.2 *Usando o gerenciador de marcadores do Firefox*



Para abrir o gerenciador de marcadores, clique em *Bookmark* → *Manage Bookmarks* (Marcador - Gerenciar Marcadores). Uma janela é aberta exibindo os marcadores. Com *New Folder* (Nova Pasta), crie uma nova pasta com um nome e uma descrição. Se você precisar de um novo marcador, clique em *New Bookmark* (Novo Marcador). Em seguida,

você poderá inserir o nome, o local, as palavras-chave e também uma descrição. A palavra-chave é um atalho para o marcador. Para adicionar o marcador recém-criado à barra lateral, marque *Load this bookmark in the sidebar* (Carregar este marcador na barra lateral).

4.3.2 Migrando marcadores

Se você usou outro browser anteriormente, provavelmente vai querer usar também suas preferências e marcadores no Firefox. No momento, é possível importar do Netscape 4.x, 6, 7, Mozilla 1.x e Opera.

Para importar suas configurações, clique em *File → Import* (Arquivo - Importar). Selecione o browser do qual as configurações serão importadas. Depois que você clicar em *Next* (Avançar), as configurações serão importadas. Localize os marcadores importados em uma pasta recém-criada, começando com `From` (De).

4.3.3 Marcadores ativos

Os marcadores ativos exibem cabeçalhos no menu de marcadores e o mantém atualizado em relação às últimas notícias. Desse modo, você pode economizar tempo com uma rápida olhada nos seus sites favoritos.

Muitos sites e blogs suportam esse formato. Um site indica isso mostrando um retângulo laranja com RSS no canto inferior direito. Clique nele e escolha *Subscribe to NAME OF THE FEED* (Inscrever-se em NOME DA ALIMENTAÇÃO). É exibida uma caixa de diálogo em que você pode selecionar o nome e o local dos marcadores ativos. Confirme com *Add* (Adicionar).

Alguns sites não informam ao Firefox que suportam a alimentação de notícias, embora realmente o façam. Para adicionar manualmente um marcador ativo, é necessário o URL da alimentação. Faça o seguinte:

Procedimento 4.1 *Adicionando manualmente um marcador ativo*

1. Abra o gerenciador de marcadores, clique em *Bookmarks → Manage Bookmarks* (Marcadores - Gerenciar Marcadores). Uma nova janela é aberta.

2 Selecione *File* → *New Live Bookmark* (Arquivo - Novo Marcador Ativo). Uma caixa de diálogo é aberta.

3 Insira um nome para o marcador ativo e adicione seu URL, por exemplo, `http://www.novell.com/newsfeeds/rss/coolsolutions.xml`. O Firefox atualiza os marcadores ativos.

4 Feche o gerenciador de marcadores.

4.4 Usando o gerenciador de downloads

Com a ajuda do gerenciador de downloads, controle os downloads atuais e anteriores. Para abrir o gerenciador de downloads, clique em *Tools* → *Downloads* (Ferramentas - Downloads). O Firefox abre uma janela com seus downloads. Ao fazer download de um arquivo, observe a barra de andamento e o arquivo atual. Pause o download e continue-o mais tarde, se necessário. Para abrir um arquivo transferido por download, clique em *Open* (Abrir). Com *Remove* (Remover), apague-o da mídia. Se precisar de informações sobre o arquivo, clique o botão direito em seu nome e escolha *Properties* (Propriedades).

Se você precisar controlar melhor o Gerenciador de Dowloads, abra a janela de configuração em *Edit* → *Preferences* (Editar - Preferências) e vá para a guia *Downloads*. Aqui, determine a pasta de download, o comportamento do gerenciador e algumas configurações de tipos de arquivo.

4.5 Personalizando o Firefox

Com a capacidade de instalar extensões, mudar temas e adicionar palavras-chave inteligentes às pesquisas online, o Firefox pode ser personalizado de forma abrangente.

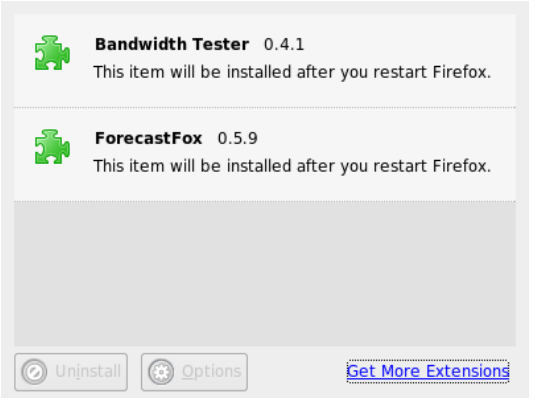
4.5.1 Extensões

O Mozilla Firefox é um aplicativo multifuncional. Isso significa que você pode fazer download de complementos, conhecidos como extensões, e instalá-los. Por exemplo,

adicione um novo gerenciador de downloads e movimentos do mouse. A vantagem é que o Firefox não fica sobrecarregado.

Para adicionar uma extensão, clique em *Tools* → *Extensions* (Ferramentas - Extensões). No canto inferior direito, clique em *Get More Extensions* (Obter Mais Extensões) para abrir a página da Web de atualização de extensões do Mozilla, na qual você pode escolher entre várias extensões disponíveis. Clique na extensão a ser instalada e, em seguida, clique no link de instalação para fazer o download e instalá-la. Quando você reiniciar o Firefox, a nova extensão estará funcionando. Também é possível encontrar várias extensões em `http://update.mozilla.org/`.

Figura 4.3 *Instalando extensões do Firefox*


Bandwidth Tester 0.4.1
This item will be installed after you restart Firefox.
ForecastFox 0.5.9
This item will be installed after you restart Firefox.
Uninstall
Options
Get More Extensions

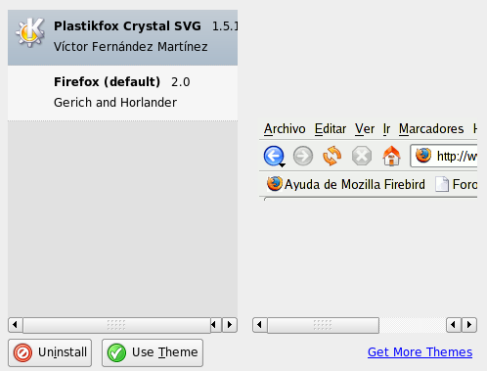
4.5.2 Mudando temas

Se você não gostar da aparência do Firefox, instale um novo *tema*. Os temas não mudam a funcionalidade do browser, somente a aparência. Durante a instalação de um tema, o Firefox solicita uma confirmação primeiro. Permita a instalação ou cancele-a. Após uma instalação bem-sucedida, é possível habilitar o novo tema.

1. Click *Tools* → *Theme* (Ferramentas - Tema).

2. Uma nova caixa de diálogo é aberta. Clique em *Get More Themes* (Mostrar Mais Temas). Se você já tiver instalado um tema, localize-o na lista, como na Figura 4.4, “Instalando temas do Firefox” (p 88).

Figura 4.4 *Instalando temas do Firefox*



3. Uma nova janela é exibida com o site `https://update.mozilla.org`.

4. Escolha um tema e clique em *Install Now* (Instalar Agora).

5. Confirme o download e a instalação.

6. Após a conclusão do download do tema, é exibida uma caixa de diálogo informando sobre a lista de temas. Ative o novo tema com *Use Theme* (Usar Tema).

7. Feche a janela e reinicie o Firefox.

Se um tema for instalado, você sempre poderá alternar para um tema diferente sem reiniciar o computador, clicando em *Tools → Themes (Ferramentas - Temas)* e, em seguida, em *Use Theme* (Usar Tema). Se você não for mais usar um tema, poderá apagá-lo na mesma caixa de diálogo com *Uninstall* (Desinstalar).

4.5.3 Adicionando palavras-chave inteligentes às pesquisas online

A pesquisa na Internet é uma das principais tarefas que um browser pode realizar. O Firefox permite que você defina suas próprias *palavras-chave inteligentes*: abreviações a serem usadas como um "comando" para pesquisa na Web. Por exemplo, se você usa

a Wikipedia com freqüência, use uma palavra-chave inteligente para simplificar essa tarefa:

1. Vá para `http://en.wikipedia.org`.

2. Uma vez aberta a página da Web, observe o campo de texto de pesquisa. Clique o botão direito do mouse e escolha *Add a Keyword for this Search* (Adicionar uma Palavra-chave para esta Pesquisa) no menu exibido.

3. A caixa de diálogo *Add Bookmark* (Adicionar Marcador) é exibida. Em *Name* (Nome), atribua um nome a esta página da Web, por exemplo, *Wikipedia (en)*.

4. Em *Keyword* (Palavra-chave), atribua uma abreviação a esta página da Web, por exemplo, *wiki*.

5. Com *Create in* (Criar em), escolha o local da entrada da seção de indicadores. Você pode colocá-la em *Quick Searches* (Pesquisas Rápidas), mas qualquer outro nível também é adequado.

6. Finalize com *Add* (Adicionar).

Você terá gerado uma nova palavra-chave. Sempre que precisar pesquisar na Wikipedia, não precisará usar o URL completo. Basta digitar `wiki Linux` para ver uma entrada sobre o Linux.

4.6 Imprimindo no Firefox

Configure a maneira como o Firefox imprime o conteúdo que exibe, usando a caixa de diálogo *Page Setup* (Configuração de Página). Clique em *File (Arquivo)* → *Page Setup* (Configuração de Página) e vá para a guia *Format & Options* (Formato e Opções) para selecionar a orientação das tarefas de impressão. Você pode ajustar manualmente ou definir o ajuste de forma automática. Para imprimir um segundo plano, selecione *Print Background (colors & images)*(Imprimir Segundo Plano (cores e imagens)). Clique na guia *Margins & Header/Footer* (Margens e Cabeçalho/Rodapé) para ajustar as margens e selecionar o que deve ser incluído nos cabeçalhos e rodapés.

Após definir as configurações, imprima uma página da Web com *File (Arquivo)* → *Print* (Imprimir). Selecione a impressora ou um arquivo no qual gravar a saída. Com *Properties* (Propriedades), defina o tamanho do papel, especifique o comando de

impressão, escolha a escala de cinza e determine as margens. Quando estiver satisfeito com as configurações, confirme com *Print* (Imprimir).

4.7 Mais informações

Obtenha mais informações sobre o Firefox na home page oficial em `http://www.mozilla.org/products/firefox/`. Consulte a ajuda integrada para saber mais sobre certas opções ou recursos.

Linphone—VoIP para o Linux Desktop

5

O Linphone é um pequeno aplicativo de telefone da Web para a área de trabalho do Linux. Ele permite que você realize chamadas entre dois computadores pela Internet. Não há necessidade de itens de hardware especiais: uma estação de trabalho padrão com uma placa de som configurada corretamente, microfone e alto-falantes ou fones de ouvido são todos os itens necessários para usar o Linphone.

5.1 Configuração do Linphone

Antes de começar a usar o Linphone, existem algumas decisões básicas a serem tomadas e algumas tarefas de configuração a completar. Primeiro, determine e configure o modo de execução do Linphone, determine o tipo de conexão a ser usado e, em seguida, inicie a configuração do Linphone (*Vá para → Preferências*) para realizar os ajustes necessários.

5.1.1 Determinação do Modo de Execução do Linphone

O Linphone pode ser executado de dois modos diferentes, dependendo do tipo de área de trabalho executado e de sua configuração.

Aplicativo normal
Depois da instalação do software do Linphone, ele pode ser iniciado pelos menus de aplicativo do GNOME e KDE ou pela linha de comando. Quando o Linphone não estiver sendo executado, as chamadas não poderão ser recebidas.

Applet do painel do GNOME
O Linphone pode ser adicionado ao painel do GNOME. Clique o botão direito do mouse em uma área vazia do painel, selecione *Adicionar ao Painel* e, em seguida, Linphone. O Linphone é então permanentemente adicionado ao painel e inicializado automaticamente no login. Enquanto você não receber chamadas, ele será executado em segundo plano. Assim que for recebida uma chamada, a janela principal será aberta e você poderá receber a chamada. Para abrir a janela principal para ligar para alguém, basta clicar no ícone do applet.

5.1.2 Determinação do tipo de conexão

Existem muitas maneiras diferentes de fazer uma chamada no Linphone. A maneira pela qual você está conectado à rede ou à Internet determina como você realizará a chamada e como alcançará a outra parte.

O Linphone utiliza o SIP (session initiation protocol) para estabelecer uma conexão com um host remoto. No SIP, cada parte é identificada pelo URL SIP :

`sip:`*`username@hostname`*

`username` é o seu login na máquina Linux e *`hostname`* é o nome do computador que você está usando. Se você é um provedor SIP, o URL será parecido com o exemplo a seguir:

`sip:`*`username@sipserver`*

`username` é o nome do usuário escolhido durante o registro em um servidor SIP. *`sipserver`* é o endereço do servidor SIP ou do seu provedor SIP. Para obter os detalhes sobre o procedimento de registro, consulte a Seção 5.1.5, “Configuração das opções SIP” (p 95) e verifique a documentação de registro do provedor. Para obter uma lista dos provedores apropriados para este propósito, consulte as páginas da Web citadas na Seção 5.8, “Mais informações” (p 102).

O URL a ser usado é determinado pelo tipo de conexão escolhida. Se optar por ligar para a outra parte diretamente sem roteamento adicional por um provedor SIP, você

deverá informar um URL do primeiro tipo. Se optar por ligar para a outra parte por meio de um servidor SIP, você deverá informar um URL do segundo tipo.

Chamada na mesma rede

Se quiser ligar para um amigo ou colega da mesma rede, você só precisará dos nomes de usuário e de host corretos para criar um URL SIP válido. O mesmo se aplica se essa pessoa quiser ligar para você. Não serão necessárias outras configurações se não houver um firewall entre você e a outra parte.

Chamadas através de redes ou pela Internet (Configuração de IP estático)

Se você estiver conectado à Internet usando um endereço IP estático, qualquer pessoa que quiser ligar para você só precisará do seu nome de usuário e nome de host ou endereço IP da sua estação de trabalho para criar um URL SIP válido, como descrito na "Chamada na mesma rede" (p 93). Se você ou a outra parte estiver sob a proteção de um firewall que filtre o tráfego de entrada e saída, abra a porta SIP (`5060`) e a porta RTP (`7078`) na máquina do firewall para habilitar o tráfego do Linphone através do firewall.

Chamadas através de redes ou pela Internet (Configuração de IP dinâmico)

Se a sua configuração não for estática, isto é, se você receber um novo endereço IP sempre que se conectar à Internet, será impossível para qualquer chamador criar um URL SIP baseado em seu nome de usuário e endereço IP. Nesses casos, utilize os serviços oferecidos por um provedor SIP ou use uma configuração DynDNS para garantir que o chamador externo consiga se conectar à máquina de host correta. Mais informações sobre o DynDNS podem ser encontradas em `http://en.wikipedia.org/wiki/Dynamic_DNS`.

Chamadas através de redes e firewalls

As máquinas escondidas atrás de um firewall não revelam o seu endereço IP pela Internet. Assim, elas não podem ser alcançadas diretamente por nenhuma pessoa que tente ligar para o usuário que estiver trabalhando nessa máquina. O Linphone suporta

ligações através de fronteiras de rede e firewalls utilizando um proxy SIP ou retransmitindo as chamadas para um provedor SIP. Consulte a Seção 5.1.5, “Configuração das opções SIP” (p 95) para obter uma descrição detalhada dos ajustes necessários para utilizar um servidor SIP externo.

5.1.3 Configuração dos parâmetros de rede

A maioria das configurações contidas na guia *Rede* não precisa de mais ajustes. Será possível fazer a sua primeira chamada sem as mudar.

Opções NAT Traversal

Habilite essa opção somente se você se encontrar em uma rede privada por trás de um firewall e se não utiliza um provedor SIP para rotear as chamadas. Marque a caixa de seleção e informe o endereço IP da máquina de firewall em notação com pontos, como `192.168.34.166`.

Propriedades RTP

O Linphone utiliza o RTP (real-time transport protocol) para transmitir os dados de áudio de suas chamadas. A porta para o RTP é definida como `7078` e não deve ser modificada, a não ser que outro aplicativo esteja usando essa porta. O parâmetro de compensação jitter é usado para controlar o número de pacotes de áudio nos quais o Linphone aplica buffer antes de realmente reproduzi-los. Ao aumentar este parâmetro, você melhora a qualidade da transmissão. Quanto mais pacotes em buffer, maior a chance de que os “atrasados” sejam reproduzidos. Por outro lado, o aumento dos pacotes em buffer também aumenta a latência, isto é, você escutará a voz de seu correspondente com um certo atraso. Quando mudar este parâmetro, equilibre cuidadosamente esses dois fatores.

Outros

Se você usar uma combinação de VoIP e telefonia fixa, poderá optar por usar a tecnologia DTMF (dual tone multiplexed frequency) para acionar determinadas ações, como a verificação remota de seu correio de voz apenas com a ajuda de algumas teclas. O Linphone suporta dois protocolos para transmissão DTMF, SIP INFO e RTP rfc2833. Se você precisar da funcionalidade da tecnologia DTMF no Linphone, escolha um provedor SIP que suporte um desses protocolos. Para obter uma lista abrangente de provedores VoIP, consulte a Seção 5.8, “Mais informações” (p 102).

5.1.4 Configuração do dispositivo de som

Depois que a sua placa de som for detectada corretamente pelo Linux, o Linphone utilizará automaticamente o dispositivo detectado como o seu dispositivo de som padrão. Não mude o valor da opção *Use sound device (Usar dispositivo de som)*. Use a opção *Recording source (Fonte de gravação)* para determinar qual fonte de gravação deve ser usada. Na maioria dos casos, essa fonte seria um microfone (`micro`). Para selecionar um som de campainha personalizado, use a opção *Browse (Pesquisar)* para escolher uma opção e teste a sua escolha utilizando a opção *Listen (Ouvir)*. Clique em *Apply (Aplicar)* para aceitar as mudanças.

5.1.5 Configuração das opções SIP

A caixa de diálogo *SIP* contém todas as definições de configuração SIP.

Porta SIP
: Determine em qual porta o agente do usuário SIP deve ser executado. A porta padrão do SIP é `5060`. Não mude a configuração padrão, a não ser que você conheça outro aplicativo ou protocolo que precise usar essa porta.

Identidade
: Qualquer pessoa que quiser ligar diretamente para você sem usar um proxy SIP ou um provedor SIP precisará conhecer o seu endereço SIP válido. O Linphone cria um endereço SIP válido para você.

Serviços remotos
: Esta lista contém um ou mais provedores de serviço SIP onde você criou uma conta do usuário. As informações sobre servidor podem ser adicionadas, modificadas ou apagadas a qualquer momento. Consulte a Adição de um proxy SIP e registro em um servidor SIP remoto (p 96) para conhecer o procedimento de registro.

Informações de autenticação
: Para registrar um servidor SIP remoto, forneça determinados dados de autenticação como senha e nome de usuário. O Linphone armazena esses dados assim que são fornecidos. Para descartar esses dados por motivos de segurança, clique em *Clear all stored authentification data (Apagar todos os dados de autenticação armazenados)*.

A lista *Remote services (Serviços remotos)* pode ser preenchida com vários endereços de proxies SIP remotos ou provedores de serviço.

Procedimento 5.1 *Adição de um proxy SIP e registro em um servidor SIP remoto*

1. Escolha um provedor SIP adequado e crie uma conta de usuário.
2. Inicie o Linphone.
3. Vá para *Ir → Preferências → SIP*.
4. Clique em *Add proxy/registrar (Adicionar proxy/registrar)* para abrir o formulário de registro.
5. Preencha os valores apropriados para as opções *Registration Period (Período de Registro)*, *SIP Identity (Identidade SIP)*, *SIP Proxy (Proxy SIP)* e *Route (Rota)*. Se estiver trabalhando por trás de um firewall, sempre selecione a opção *Send registration (Enviar registro)* e digite um valor apropriado para a opção *Registration Period (Período de Registro)*. Esta ação envia novamente os dados de registro originais depois de um determinado tempo para manter o firewall aberto nas portas necessárias ao Linphone. Caso contrário, essas portas seriam fechadas automaticamente se o firewall não recebesse mais pacotes deste tipo. Também é necessário enviar novamente os dados de registro para manter o servidor SIP informado sobre o status atual da conexão e o local do chamador. Para a opção *SIP identity (Identidade SIP)* digite o URL SIP que deve ser usado para as chamadas locais. Para usar este servidor também como um proxy SIP, digite os mesmos dados para a opção *SIP Proxy (Proxy SIP)*. Finalmente, adicione uma rota opcional, se necessário, e deixe a caixa de diálogo com *OK*.

5.1.6 Configuração dos codecs de áudio

O Linphone suporta vários codecs para a transmissão de dados de voz. Defina o seu tipo de conexão e escolha seus codecs preferidos na janela de lista. Os codecs que não são adequados para o seu tipo de conexão atual ficam em vermelho e não podem ser selecionados.

5.2 Teste do Linphone

Verifique a configuração do Linphone utilizando o `sipomatic`, um pequeno programa de testes que pode responder a chamadas feitas do Linphone.

Procedimento 5.2 *Teste de configuração do Linphone*

1. Abra um terminal.
2. Digite `sipomatic` no prompt da linha de comando.
3. Inicie o Linphone.
4. Digite `sip:robot@127.0.0.1:5064` como o *endereço SIP* e clique em *Call or Answer (Ligar ou Atender)*.
5. Se o Linphone estiver configurado corretamente, você ouvirá um telefone tocando e, após um curto período de tempo, um pequeno anúncio.

Se você completar este procedimento corretamente, poderá ter certeza de que suas configurações de áudio e de rede estão funcionando. Se este teste falhar, verifique se o seu dispositivo de som está configurado corretamente e se o nível de reprodução está definido para um valor razoável. Se ainda não conseguir ouvir nada, verifique a configuração da rede, incluindo os números de porta para SIP e RTP. Se nenhum outro aplicativo ou protocolo utilizar as portas padrão para eles, como proposto pelo Linphone, considere a opção de mudar as portas e tentar novamente.

5.3 Realização de chamada

Depois que o Linphone estiver configurado corretamente, será muito fácil fazer uma chamada. Dependendo do tipo de chamada (consulte a Seção 5.1.2, “Determinação do tipo de conexão” (p 92) para obter referências), os procedimentos de chamada são um pouco diferentes.

1. Inicie o Linphone utilizando o menu ou uma linha de comando.
2. Digite o endereço SIP da outra parte no prompt *SIP address (Endereço SIP)*. O endereço deve ser parecido com `sip:username@domainname` ou

`username@hostname`, para chamadas diretas locais, ou `username@sipserver` ou `userid@sipserver`, para chamadas em proxy ou chamadas que utilizam os serviços de um provedor SIP.

3. Se estiver utilizando um provedor de serviço SIP ou um proxy, selecione o proxy ou provedor apropriado em *Proxy to use (Proxy a ser utilizado)* e forneça a data de autenticação solicitada por este proxy.

4. Clique em *Call or Answer (Ligar ou Atender)* e espere que a outra parte atenda ao telefone.

5. Assim que terminar ou quiser terminar a chamada, clique em *Release or Refuse (Liberar ou Recusar)* e saia do Linphone.

Se precisar ajustar os parâmetros de som durante a chamada, clique em *Show more (Mais informações)* para exibir quatro guias contendo mais opções. A primeira contém as opções *Sound (Som)* para o *Playback level (Nível de reprodução)* e *Recording level (Nível de gravação)*. Use os controles deslizantes para ajustar os volumes de acordo com a sua necessidade.

A guia *Presence (Presença)* permite que você defina o seu status online. Essas informações podem ser retransmitidas para qualquer pessoa que tentar entrar em contato com você. Se você está fora permanentemente e deseja informar isso à pessoa que ligar, apenas marque a opção *Away (Ausente)*. Se você está apenas ocupado, mas deseja que a outra parte ligue novamente, marque a opção *Busy, I'll be back in ... min (Ocupado, estarei de volta em ... min)* e especifique por quanto tempo não poderá ser contatado. Quando estiver disponível novamente, retorne o status para o padrão (*Reachable (Disponível)*). A *Subscribe Policy (Política de Inscrição)*, definida no bloco de endereços, como descrito na Seção 5.5, “O Bloco de Endereços” (p 99), determina se a outra parte pode verificar o seu status online. Se alguma pessoa listada em seu bloco de endereços publicar o status online dela, você poderá monitorá-la utilizando a guia *My online friends (Meus amigos online)*.

A guia *DTMF* pode ser usada para informar os códigos DTMF para verificação de correio de voz. Para verificar o seu correio de voz, informe o endereço SIP adequado e use o teclado na guia *DTMF* para digitar o código do correio de voz. Finalmente, clique em *Call or Answer (Ligar ou Atender)* como se fosse fazer uma ligação normal.

5.4 Para atender uma chamada

Dependendo do modo de execução selecionado para o Linphone, existem várias maneiras de perceber o recebimento de uma chamada:

Aplicativo normal
: As chamadas só podem ser recebidas e atendidas se o Linphone já estiver sendo executado. Você escutará um som de campainha no fone de ouvido ou alto-falante. Se o Linphone não estiver sendo executado, a chamada não poderá ser recebida.

Applet do painel do GNOME
: Normalmente, o applet do painel do Linphone seria executado silenciosamente, sem dar nenhum sinal de sua existência. Isso muda assim que uma chamada é recebida: a janela principal do Linphone é aberta e você escuta um som de campainha em seu fone de ouvido ou nos alto-falantes.

Assim que você perceber o recebimento de uma chamada, clique em *Call or Answer (Ligar ou Atender)* para atender ao telefone e começar a falar. Se não quiser aceitar a ligação, clique em *Release of Refuse (Liberação de Recusa)*.

5.5 O Bloco de Endereços

Com o Linphone, você pode gerenciar os seus contatos SIP. Inicie o bloco de endereços em *Go (Ir) → Address book (Bloco de endereços)*. Uma janela de lista vazia é exibida. Clique em *Add (Adicionar)* para adicionar um contato.

As entradas a seguir precisam ser feitas para um contato válido:

Name (Nome)
: Digite o nome do contato. Pode ser o nome completo ou um apelido. Escolha algo que o faça lembrar dessa pessoa. Se você quiser ver o status online da pessoa, esse nome será exibido na guia *My online friends (Meus amigos online)* da janela principal.

SIP Address (Endereço SIP)
: Digite um endereço SIP válido para o contato.

Proxy to Use (Proxy a ser usado)
Se necessário, informe o proxy a ser usado para esta conexão em particular. Na maioria dos casos, este seria apenas o endereço SIP do servidor SIP que você usa.

Subscribe Policy (Política de Inscrição)
A sua política de inscrição determina se a sua presença ou ausência pode ser rastreada por terceiros.

Para ligar para qualquer contado do bloco de endereços, selecione o contato com o mouse, clique em *Select (Selecionar)* para fazer com que o endereço seja exibido no campo de endereço da janela principal e inicie a chamada com a opção *Call or Answer (Ligar ou Atender)*, como de costume.

5.6 Solução de problemas

Tentei ligar para uma pessoa, mas não consegui estabelecer uma conexão.
Existem vários motivos que podem causar a falha de uma ligação:

A sua conexão com a Internet caiu.
Como o Liphone utiliza a Internet para retransmitir as suas chamadas, verifique se o computador está corretamente conectado e configurado para a Internet. Para fazer isso, basta tentar exibir uma página da Web utilizando o browser. Se a conexão com a Internet funcionar, o problema pode ser com a outra parte.

A pessoa para quem você está ligando não pode ser contactada.
Se a outra parte recusar a sua chamada, você não será conectado. Se o Linphone não estiver sendo executado na máquina da outra pessoa quando você ligar para ela, você não será conectado. Se a conexão com a Internet da outra parte tiver caído, não será possível fazer a conexão.

Parece que a minha ligação foi completada, mas eu não consigo escutar nada.
Primeiro, verifique se o seu dispositivo de som está configurado corretamente. Faça isso inicializando outro aplicativo que utiliza a saída de som, como um leitor de mídia. Verifique se o Linphone tem permissões suficientes para abrir esse dispositivo. Feche todos os outros programas que utilizam o dispositivo de som para evitar conflitos de recursos.

Se as verificações acima forem bem-sucedidas, mas você ainda não conseguir escutar nada, aumente os níveis de gravação e reprodução na guia *Som*.

A saída de som em ambas as extremidades soa estranhamente cortada.
Tente ajustar o buffer de jitter utilizando as *RTP properties (Propriedades RTP)* em *Preferences (Preferências) → Network (Rede)* para compensar os pacotes de voz atrasados. Quando fizer isso, lembre-se de que esse processo aumenta a latência.

O DTMF não funciona.
Você tentou verificar o correio de voz utilizando o teclado numérico DTMF, mas a conexão não pôde ser estabelecida. Existem três tipos diferentes de protocolos usados para a transmissão de dados DTMF, mas somente dois desses protocolos são suportados pelo Linphone (SIP INFO e RTP rfc2833). Verifique com seu provedor se ele suporta uma dessas opções. O protocolo padrão usado pelo Linphone é rfc2833, mas se ele falhar, você pode definir o protocolo para SIP INFO em *Preferences (Preferências) → Network (Rede) → Other (Outros)*. Se ele não funcionar com nenhuma das opções, a transmissão não poderá ser realizada com o Linphone.

5.7 Glossário

Veja algumas explicações resumidas dos termos técnicos e protocolos mais importantes mencionados neste documento:

VoIP
VoIP corresponde a *voice over Internet protocol*. Esta tecnologia possibilita a transmissão de ligações comuns de telefone pela Internet utilizando rotas packet-linked. As informações de voz são enviadas em pacotes distintos, como qualquer outro tipo de dados transmitido pela Internet via IP.

SIP
SIP corresponde a *session initiation protocol*. Este protocolo é usado para estabelecer sessões de mídia pelas redes. Em um contexto do Linphone, o SIP é a mágica que aciona a campainha na máquina da pessoa para quem você liga, inicia e também termina a ligação assim que uma das partes decide desligar. A transmissão real de voz é tratada pelo RTP.

RTP
RTP corresponde a *real-time transport protocol*. Ele possibilita o transporte de streaming de mídia pelas redes e funciona sobre o UDP. Os dados são transmitidos através de pacotes distintos que são numerados e que carregam uma marcação de horário para permitir o seqüenciamento e a detecção corretos de pacotes perdidos.

DTMF
: Um codificador DTMF, como um telefone normal, utiliza pares de tons para representar as várias teclas. Cada tecla é associada a uma combinação exclusiva entre um tom alto e outro baixo. Um decodificador então traduz essas combinações entre tom e toque para números. O Linphone suporta os sinais DTMF para acionar ações remotas, como a verificação de correio de voz.

codec
: Codecs são algoritmos especialmente desenvolvidos para compactar dados de áudio e vídeo.

jitter
: O Jitter é a variação da latência (atraso) em uma conexão. Os dispositivos de áudio ou sistemas voltados para a conexão, como o ISDN ou o PSTN, precisam de um streaming contínuo de dados. Para compensar isto, os terminais e gateways VoIP implementam um buffer de jitter que coleta os pacotes antes de retransmiti-los para outros dispositivos de áudio ou linhas voltadas para conexão (como o ISDN). O aumento do tamanho do buffer de jitter diminui a probabilidade de perda de dados, mas a latência da conexão aumenta.

5.8 Mais informações

Para obter informações gerais sobre VoIP, verifique a seção VoIP Wiki em `http://voip-info.org/tiki-index.php`. Para obter uma lista abrangente de provedores que oferecem serviços VoIP em seu país, consulte a `http://voip-info.org/wiki-VOIP+Service+Providers+Residential`.

6 Criptografia com KGpg

O KGpg é um componente importante da infra-estrutura de criptografia do sistema. Com a ajuda desse programa, é possível gerar e gerenciar todas as chaves necessárias, usar a função de editor para criar e criptografar arquivos rapidamente, ou usar o applet no painel para criptografar ou descriptografar com o recurso de arrastar e soltar. Outros programas, como os de e-mail (Kontact ou Evolution), acessam os dados de chaves para processar conteúdos assinados ou criptografados. Este capítulo abrange as funções básicas necessárias para o trabalho diário com arquivos criptografados.

6.1 Gerando um novo par de chaves

Para poder trocar mensagens criptografadas com outros usuários, primeiro gere seu próprio par de chaves. Uma das chaves, a *chave pública*, será distribuída a seus parceiros de comunicação, que poderão usá-la para criptografar os arquivos ou mensagens de e-mail que enviarem. A outra parte do par de chaves, a *chave privada*, será usada para decodificar o conteúdo criptografado.

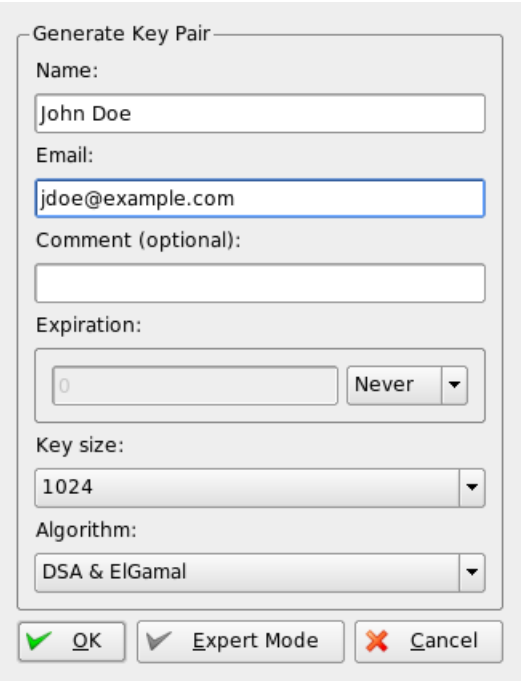
IMPORTANTE: Chave privada versus chave pública

A chave pública se destina à esfera pública e deve ser distribuída a todos os seus parceiros de comunicação. No entanto, só você deve ter acesso à chave privada. Não permita que outros usuários tenham acesso a esses dados.

Inicie o KGpg no menu principal, selecionando *Utilitários* → *KGpg*, ou digite `kgpg` na linha de comando. Quando você iniciar o programa pela primeira vez, um assistente será exibido para orientá-lo na configuração. Siga as instruções até o ponto em que

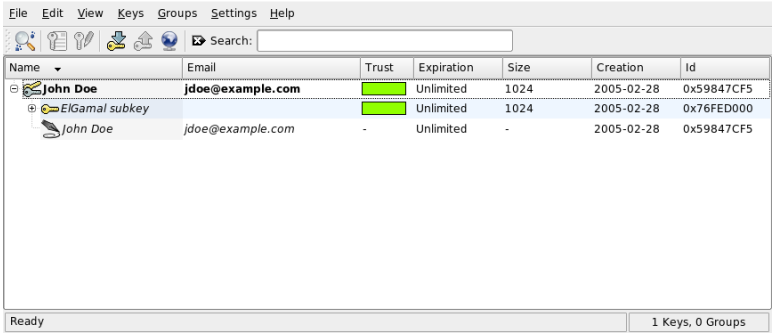
estiver pronto para criar uma chave. Insira um nome, um endereço de e-mail e, opcionalmente, um comentário. Se você não estiver satisfeito com as configurações padrão fornecidas, defina também o prazo de validade para a chave, o tamanho da chave e o algoritmo de criptografia usado. Consulte Figura 6.1, “KGpg: Criando uma chave” (p 104).

Figura 6.1 *KGpg: Criando uma chave*



Confirme as configurações com *OK*. A próxima caixa de diálogo solicita que você digite a senha duas vezes. O programa então gera um par de chaves e exibe um resumo. É recomendável salvar ou imprimir o certificado de revogação na hora. Tal certificado será necessário caso você esqueça a senha de sua chave privada e tenha que revogá-la. Depois de confirmar com *OK*, o KGpg exibirá a janela principal. Consulte Figura 6.2, “Gerenciador de chaves” (p 105).

Figura 6.2 *Gerenciador de chaves*


File Edit View Keys Groups Settings Help
Search:
Name Email Trust Expiration Size Creation Id
John Doe jdoe@example.com Unlimited 1024 2005-02-28 0x59847CF5
ElGamal subkey Unlimited 1024 2005-02-28 0x76FED000
John Doe jdoe@example.com - Unlimited - 2005-02-28 0x59847CF5
Ready
1 Keys, 0 Groups

6.2 Exportando a chave pública

Após gerar o novo par de chaves, disponibilize a chave pública para todos os usuários. Esse procedimento permitirá que eles usem o par para criptografar ou assinar as mensagens ou arquivos que enviarem a você. Para disponibilizar a chave pública para outras pessoas, selecione *Chaves → Exportar Chave(s) Pública(s)*. A caixa de diálogo aberta oferece quatro opções:

E-mail
: Sua chave pública será enviada por e-mail ao destinatário que você escolher. Se você ativar essa opção e confirmar com *OK*, será exibida a caixa de diálogo para criação de nova mensagem de e-mail com KMail. Especifique o destinatário e clique em *Enviar*. O destinatário receberá sua chave e poderá enviar-lhe conteúdo criptografado.

Área de transferência
: Você poderá usar essa opção para informar sua chave pública antes de continuar a processá-la.

Servidor de chave padrão
: Para disponibilizar sua chave pública para um número maior de pessoas, exporte-a para um dos servidores de chaves da Internet. Para obter mais informações, consulteSeção 6.4, “Caixa de diálogo do servidor de chaves” (p 107).

Arquivo

Se você preferir distribuir sua chave na forma de arquivo em um meio de dados em vez de enviá-la por e-mail, clique nessa opção, confirme ou mude o caminho e o nome do arquivo e clique em *OK*.

6.3 Importando chaves

Se você receber uma chave em um arquivo (como anexo de e-mail, por exemplo), integre-a ao seu chaveiro usando o recurso *Importar Chave* e use-a nas comunicações criptografadas com o remetente. O procedimento é semelhante ao da exportação de chaves, já descrito.

6.3.1 Assinando chaves

As chaves podem ser assinadas como qualquer outro arquivo para garantir sua autenticidade e integridade. Se você tiver certeza absoluta de que uma chave importada pertence à pessoa especificada como proprietário, expresse sua confiança na autenticidade da chave, assinando-a.

IMPORTANTE: Estabelecendo uma rede de confiança

A comunicação criptografada só é segura enquanto você consegue associar as chaves públicas em circulação ao usuário específico. Ao cruzar as referências das chaves e assiná-las, você contribui para o estabelecimento de uma rede de confiança.

Na lista de chaves, selecione a chave a ser assinada. Selecione *Chaves → Assinar Chaves* Na caixa de diálogo seguinte, designe a chave privada a ser usada com a assinatura. Um alerta o lembrará de verificar a autenticidade da chave antes de assiná-la. Se essa verificação já tiver sido feita, clique em *Continuar* e digite a senha da chave privada selecionada na próxima etapa. Agora, outros usuários podem verificar a assinatura usando sua chave pública.

6.3.2 Confiando em chaves

Normalmente, o programa correspondente pergunta se você confia na chave (se você supõe que seja realmente usada por seu proprietário autorizado). Isso ocorre sempre que for necessário descriptografar uma mensagem ou verificar uma assinatura. Para evitar essa situação, edite o nível de confiança da chave recém-importada.

Clique o botão direito do mouse na nova chave importada para acessar um pequeno menu de contexto do gerenciamento de chaves. Selecione *Editar Chave no Terminal*. O KGpg abrirá um console de texto no qual você poderá definir o nível de confiança por meio de alguns comandos.

No prompt do console de texto (`Command >`), digite `trust`. Em uma escala entre `1` (sem confiança) e `5` (confiança total), faça uma estimativa do quanto você confia que os assinantes da chave importada tenham verificado a real identidade do proprietário da chave. Digite o valor selecionado no prompt (`Your decision?`). Se tiver realmente certeza sobre a confiabilidade do assinante, digite `5`. Responda a pergunta digitando `y`. Finalmente, digite `quit` para sair do console e retornar à lista de chaves. A chave agora tem o nível de confiança `Definitivo`.

O nível de confiança das chaves de seu chaveiro é indicado por uma barra colorida ao lado do nome da chave. Quanto mais baixo for o nível de confiança, menos você confia que o assinante da chave tenha verificado a identidade das chaves assinadas. Você pode estar totalmente seguro sobre a identidade do assinante, mas ainda assim ele pode ter preguiça de verificar a identidade de outras pessoas antes de assinar as chaves. Portanto, você pode continuar confiando nele e na respectiva chave, mas atribua níveis de confiança mais baixos às chaves assinadas por ele. O objetivo do nível de confiança é apenas servir de lembrete. Ele não aciona qualquer ação automática pelo KGpg.

6.4 Caixa de diálogo do servidor de chaves

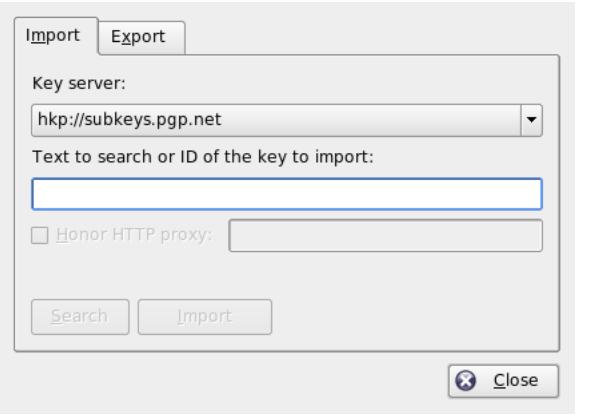
Vários servidores baseados em Internet oferecem chaves públicas de vários usuários. Para estabelecer comunicação criptografada com um grande número de usuários, use esses servidores para distribuir sua chave pública. Para isso, exporte sua chave pública para um desses servidores. Da mesma forma, o KGpg permite que você procure as

chaves de determinadas pessoas em algum desses servidores e as importe. Abra a caixa de diálogo do servidor da chave em *Arquivo → Caixa de Diálogo do Servidor da Chave*.

6.4.1 Importando uma chave de um servidor de chaves

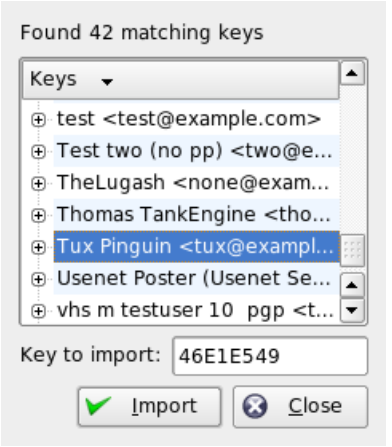
Usando a guia *Importar* da caixa de diálogo do servidor de chaves, importe chaves públicas de um dos servidores de chaves baseados na Internet. Use o menu suspenso para selecionar um dos servidores de chaves pré-configurados e inserir uma string de busca (endereço de e-mail do parceiro de comunicação) ou o ID da chave a ser procurada. Quando você clica em *Pesquisar*, o sistema se conecta à Internet e procura no servidor de chaves especificado uma chave que corresponda às especificações. Consulte a Figura 6.3, “Tela de pesquisa para importação de chave” (p 108).

Figura 6.3 *Tela de pesquisa para importação de chave*



Se a pesquisa no servidor de chaves for bem-sucedida, em uma nova janela, será exibida uma lista de todas as entradas recuperadas do servidor. Selecione a chave a ser incluída no seu chaveiro e clique em *Importar*. Consulte Figura 6.4, “Resultados e importação” (p 109). Confirme a mensagem seguinte com *OK* e saia da caixa de diálogo do servidor de chaves com *Fechar*. A chave importada aparecerá na visão geral principal do gerenciador de chaves e estará pronta para uso.

Figura 6.4 *Resultados e importação*



6.4.2 Exportando suas chaves para um servidor de chaves

Para exportar sua chave para um dos servidores acessíveis gratuitamente na Internet, selecione *Exportar* na caixa de diálogo do servidor de chaves. Designe o servidor de destino e a chave a ser exportada em dois menus suspensos. Em seguida, inicie a exportação clicando em *Exportar*.

Figura 6.5 *Exportando uma chave para um servidor de chaves*

6.5 Criptografia de texto e arquivo

O KGpg também oferece a possibilidade de criptografar texto ou conteúdo da área de transferência. Clique no ícone de cadeado para encontrar as opções *Criptografar Área de Transferência* e *Descriptografar Área de Transferência*, bem como a opção para abrir o editor integrado.

6.5.1 Criptografando e descriptografando a área de transferência

Os arquivos copiados para a área de transferência podem ser facilmente criptografados. Abra a visão geral da função clicando no ícone do KGpg. Selecione *Criptografar Área de Transferência* e designe a chave a ser usada. Uma mensagem de status sobre o procedimento de criptografia será exibida na área de trabalho. Nesse momento, o conteúdo criptografado pode ser acessado na área de transferência conforme necessário. Descriptografar o conteúdo da área de transferência também é uma tarefa fácil. Basta abrir o menu no painel, selecionar *Descriptografar Área de Transferência* e digitar a senha associada à chave privada. A versão descriptografada estará disponível para processamento na área de transferência e no editor do KGpg.

6.5.2 Arrastando e soltando para criptografar e descriptografar

Para criptografar ou descriptografar arquivos, clique nos ícones da área de trabalho ou no gerenciador de arquivos, arraste-os até o cadeado no painel e solte-os sobre ele. Se o arquivo não estiver criptografado, o KGpg solicitará a chave a ser usada. Assim que você selecionar uma chave, o arquivo será criptografado e não serão exibidas outras mensagens. No gerenciador de arquivos, os arquivos criptografados são designados com o sufixo `.asc` e com o ícone de cadeado. Para descriptografar esses arquivos, clique em um de seus ícones, arraste-os até o símbolo KGpg no painel e solte-os. Decida se o arquivo deverá ser descriptografado e gravado ou exibido no editor.

6.5.3 O editor do KGpg

Em vez de criar conteúdo para criptografia em um editor externo e, depois, criptografar o arquivo usando um dos métodos descritos acima, você pode usar o editor integrado do KGpg para criar o arquivo. Abra o editor selecionando *Abrir Editor* no menu de contexto, digite o texto desejado e clique em *Criptografar*. Em seguida, selecione a chave a ser usada e conclua o procedimento de criptografia. Para descriptografar arquivos, use opção *Descriptografar* e digite a senha associada à chave.

Gerar e verificar assinaturas é tão fácil quando criptografar diretamente no editor. Vá para *Assinatura* → *Gerar Assinatura* e selecione o arquivo a ser assinado na caixa de diálogo. Em seguida, designe a chave privada a ser usada e digite a senha associada. O KGpg informará sobre a geração bem-sucedida da assinatura. Os arquivos também podem ser assinados no editor com um simples clique em *Assinar/Verificar*. Para verificar um arquivo assinado, vá para *Assinatura* → *Verificar Assinatura* e selecione o arquivo a ser verificado na caixa de diálogo seguinte. Depois que você confirmar a seleção, o KGpg verificará a assinatura e reportará o resultado da operação. Outra possibilidade é carregar o arquivo assinado no editor e clicar em *Assinar/Verificar*.

6.6 Para obter mais informações

Para obter informações teóricas sobre o método de criptografia, consulte a breve e clara apresentação nas páginas do projeto GnuPG em `http://www.gnupg.org/documentation/howtos.html.en`. Este documento também fornece uma lista com outras fontes de informação.

Parte III Multimídia

7 Som no Linux

O Linux contém uma grande variedade de aplicativos de som e multimídia. Alguns desses aplicativos fazem parte de um dos principais ambientes de área de trabalho. Com os aplicativos descritos aqui, controle o volume e equilíbrio da reprodução, reproduza CDs e arquivos de música, e grave e compacte seus próprios dados de áudio.

7.1 Mixers

Os mixers são um meio conveniente de controlar o volume e o equilíbrio da saída e da entrada de som nos computadores. A principal diferença entre os diversos mixers é a aparência externa da interface do usuário. Entretanto, existe uma série de mixers que são designados para um hardware específico. Um exemplo é o envy24control, mixer do Envy 24 e chip de som. Outro é o hdspmixer, que se destina às placas RME Hammerfall. Dos mixers disponíveis, escolha aquele que melhor atenda às suas necessidades.

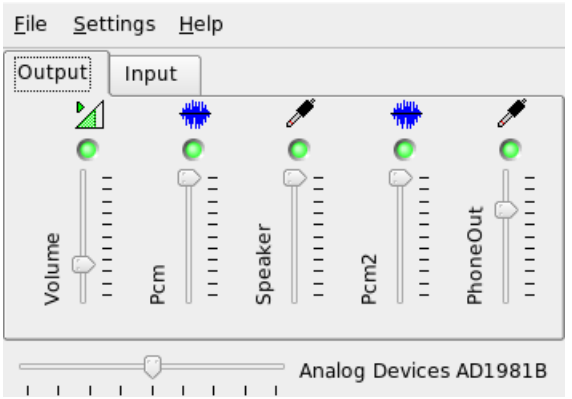
DICA: Teste seu mixer

Geralmente, recomendamos abrir o aplicativo de mixagem antes de abrir outros aplicativos de som. Use o mixer para testar e ajustar as configurações de controle de entrada e saída da placa de som.

7.1.1 Applet KDE Mixer

O KMix é o aplicativo de mixagem do KDE. Ele é integrado ao painel do KDE assim como um pequeno applet do painel localizado na bandeja do sistema. Clique no ícone do painel para ajustar o volume dos alto-falantes com um controle deslizante. Se você clicar o botão direito do mouse em um ícone, o menu de contexto do KMix será exibido. Selecione *Sem Áudio* para desligar a saída de som. O ícone do painel, em seguida, muda seu aspecto Quando você clica em *Sem Áudio* novamente, o volume é ativado. Para ajustar suas configurações de som, selecione *Mostrar Janela de Mixagem* e configure *Saída*, *Entrada* e *Switches*. Cada um dos dispositivos apresentados ali possui seu próprio menu de contexto que é aberto clicando-se o botão direito do mouse no ícone do dispositivo. Você pode desativar ou ocultar cada um deles separadamente.

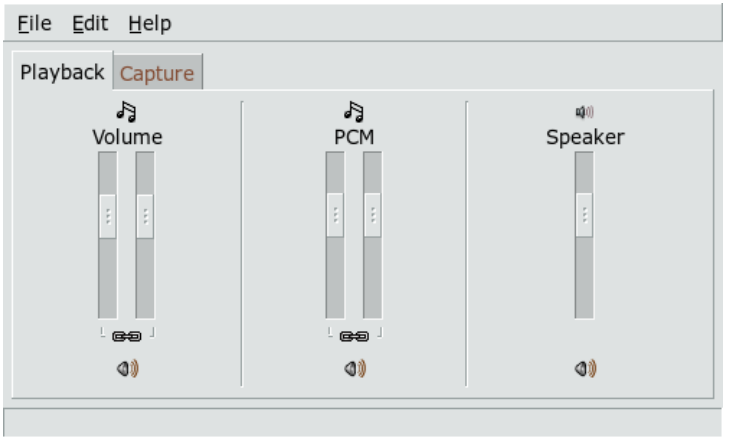
Figura 7.1 *Mixer KMix*



7.1.2 Applet GNOME Mixer

GMix, o applet de controle de volume da área de trabalho do GNOME, é integrado ao painel do GNOME. Clique no ícone do painel para ajustar o volume dos alto-falantes com um simples controle deslizante. Para desligar a saída de som, clique o botão direito do mouse no ícone e selecione *Sem Áudio*. O ícone do controle de volume, em seguida, modifica seu aspecto. Para ativar a saída de som, clique o botão direito do mouse no ícone novamente e selecione *Sem Áudio* no menu. Selecione *Abrir Controle de Volume* para acessar os recursos mais avançados de mixagem, mostrados na Figura 7.2, “Applet GNOME Mixer” (p 117). Cada dispositivo de som possui sua própria guia de mixagem.

Figura 7.2 *Applet GNOME Mixer*



7.1.3 alsamixer

O alsamixer pode ser executado a partir da linha de comando, fora do ambiente X, de modo que é inteiramente controlado por meio de atalhos do teclado. Uma janela alsamixer sempre consiste nos seguintes elementos: uma linha superior contendo informações básicas sobre a placa e o tipo de chip, o tipo de visualização selecionado e o item de mixagem. Em seguida, as barras de volume abaixo da área de informações. Use ← e → para percorrer à esquerda ou direita se os controles não puderem ser exibidos em uma tela. Os nomes dos controles aparecem abaixo deles e o controle atualmente selecionado está na cor vermelha. Alterne entre o status desativado e ativado de qualquer controle de mixagem usando M. Um controle desativado requer a inscrição *MM* abaixo do nome. Qualquer controle dotado de recursos de captura (gravação) possui um flag de captura vermelho.

O alsamixer possui três modos de visualização diferentes: *Reprodução*, *Captura* e *Todos*. Por padrão, o alsamixer é iniciado em modo de *reprodução*, exibindo somente os controles de mixagem relevantes para a reprodução (Volume Master, PCM, CD, etc.). *Captura* exibe somente os controles usados para a gravação. *Todos* exibe todos os controles disponíveis. Alterne entre os modos de visualização usando F3, F4 e F5.

Selecione os canais com → e ← ou N e P. Use ↑ e ↓ ou + e - para aumentar e diminuir o volume. Os canais estéreo podem ser controlados de maneira independente, usando Q, W e E para aumentar o volume e Z, X e C para diminuí-lo. As teclas

numéricas entre 0 e 9 podem ser usadas para mudar o volume absoluto com rapidez. Essas teclas correspondem à faixa de zero a noventa por cento do volume máximo.

7.1.4 Aparência e funcionamento dos aplicativos de mixagem

A aparência e o funcionamento dos aplicativos de mixagem dependerá do tipo de placa de som usada. Alguns drivers, como o SB Live!, possuem diversos elementos de mixagem controláveis (sintonizáveis), ao passo que os drivers de placas de som profissionais podem ter elementos com nomes totalmente diferentes.

Chip de som na placa

A maioria dos chips de som PCI em placa se baseia no padrão AC97 codec. *Mestre* controla o volume principal dos alto-falantes frontais. *Surround*, *Central* e *LFE* controlam os alto-falantes traseiros, centrais e bass-boost. Cada um desses possui um botão Mudo. Além disso, algumas placas possuem volumes individuais para *Fone de Ouvido* e *Master Mono*. Este último é usado com o alto-falante embutido em alguns laptops.

PCM controla o nível do volume interno da reprodução digital WAVE. PCM é o acrônimo de Pulse Code Modulation (Modulação de Código de Pulso), um dos formatos dos sinais digitais. Esse controle também possui um switch de áudio individual.

Outros volumes, como *CD*, *Linha*, *Microfone* e *Aux*, controlam o volume de loopback da entrada correspondente para a saída principal. Eles não influenciam o nível de gravação, somente os volumes de reprodução.

Para gravar, ligue o switch *Capturar*. Esse é o switch de gravação mestre. O volume *Capturar* é o ganho de entrada para a gravação. Por padrão, esse switch é definido com o valor zero. Escolha uma fonte de gravação, como *Linha* ou *Microfone*. Como a fonte de gravação é exclusiva, você não pode escolher duas fontes ao mesmo tempo. *Mix* é uma fonte de gravação especial. É possível gravar o sinal em reprodução a partir dessa fonte.

Dependendo do chip codec AC97, efeitos especiais, como 3D ou baixo/agudo, também estão disponíveis.

Família SoundBlaster Live! e Audigy

O SoundBlaster Live! e o SB Audigy1 possuem diversos controles de mixagem para o chip codec AC97 e o motor DSP. Além dos controles já descritos, eles dispõem dos volumes *Wave*, *Música* e *AC97* para controlar o roteamento de sinais internos e a atenuação de mixagem PCM, WaveTable MIDI e AC97. Mantenha o volume em 100% para ouvir todos esses elementos. O SB Audigy2 (dependendo do modelo) possui menos controles do que o SB Live, mas ainda assim dispõe dos controles *Wave* e *Música*.

A gravação no SB Live é semelhante ao chip em placa. Você pode escolher *Wave* e *Música* como a fonte de gravação adicional para gravar os sinais PCM e WaveTable reproduzidos.

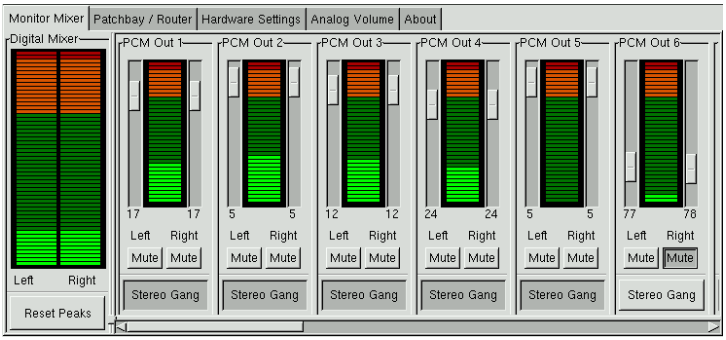
Dispositivos de áudio USB

Os dispositivos de áudio USB geralmente possuem um número pequeno de controles de mixagem. Às vezes, chegam a não ter controle algum. A maioria dos dispositivos possui um switch de controle *Mestre* ou *PCM* para ajustar o volume de reprodução.

7.1.5 Mixer para o chip de som Envy24

O envy24control é um aplicativo de mixagem para placas de som que usa o chip Envy24 (ice1712). A flexibilidade do chip Envy24 pode resultar em diferentes funcionalidades em várias placas de som. Para obter os detalhes mais recentes sobre esse chip de som, consulte `/usr/share/doc/packages/alsa-tools/envy24control`.

Figura 7.3 *Monitor e mixer digital do envy24control*



O *Mixer Monitor* do envy24control mostra os níveis de sinais que podem ser mixados digitalmente na placa de som. Os sinais designados como *Saída PCM* são gerados por aplicativos que enviam dados PCM à placa de som. Os sinais das entradas analógicas são mostrados em *Entrada de H/W*. As entradas *S/PDIF* são mostradas à direita na tela. Ajuste os níveis de entrada e saída dos canais analógicos em *Volume Analógico*.

Use os controles deslizantes do *Mixer Monitor* para fazer a mixagem digital. Os respectivos níveis são exibidos em *Mixer Digital*. Para cada canal de saída, *Patchbay* contém uma linha de botões de opção para a seleção da fonte de canal desejada.

Ajuste a amplificação dos conversores de analógico para digital e vice-versa em *Volume Analógico*. Use os controles deslizantes *DAC* com os canais de saída e os controles deslizantes *ADC* com os canais de entrada.

As configurações do canal S/PDIF são efetuadas na guia *Configurações de Hardware*. O chip Envy24 reage a alterações de volume com um atraso a ser configurado em *Alteração de Volume*.

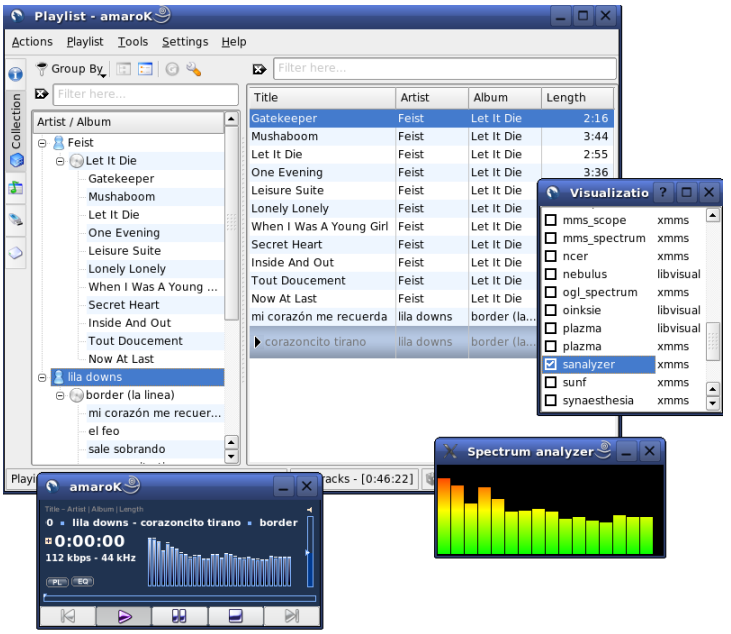
7.2 Leitores multimídia

7.2.1 amaroK

O leitor de mídia amaroK aceita vários formatos de áudio e reproduz transmissões de streaming de áudio de estações de rádio da Internet. O programa usa todos os tipos de arquivos suportados pelo servidor de som, agindo como backend, atualmente aRts ou GStreamer.

Na primeira inicialização, o amaroK inicia um *Assistente de Primeira Execução*, que é útil para a configuração do amaroK. Na primeira etapa, configure a aparência do amaroK de sua preferência. Opte pela exibição do leitor e da lista de reprodução em janelas separadas (veja a Figura 7.4, “Leitor de mídia amaroK” (p 121)) ou combine sua funcionalidade em uma única janela. Na segunda etapa, determine o local em que o amaroK deve buscar sua coleção de música. O amaroK procura mídia reproduzível nessas pastas. Por padrão, o amaroK é configurado para explorar as pastas selecionadas recursivamente (de modo a incluir todos os subdiretórios na busca), monitorar mudanças no conteúdo dos diretórios selecionados e importar as eventuais listas de reprodução encontradas. Para modificar as configurações feitas com o assistente posteriormente, inicie o assistente outra vez em *Ferramentas → Assistente de Primeira Execução*.

Figura 7.4 *Leitor de mídia amaroK*



Gerenciando listas de reprodução

Na inicialização, o amaroK busca arquivos multimídia no sistema de arquivos de acordo com as configurações feitas com o assistente. O canto direito da janela da lista de reprodução relaciona as listas encontradas. Reproduza os títulos listados na ordem desejada. Se nenhuma lista for encontrada, crie uma. A melhor forma de fazer isso é usar a barra lateral à esquerda da janela. Mais à esquerda, há algumas guias que podem ser usadas para abrir diversas telas. Em cada uma dessas telas, arraste títulos individuais ou diretórios inteiros e solte-os na lista de reprodução para incluí-los. Veja abaixo uma descrição do funcionamento de cada guia.

Contexto

Nesta guia, veja informações sobre sua coleção e sobre o artista atual. Por exemplo, a tela contém informações sobre seus títulos favoritos, novos títulos adicionados à coleção e outros detalhes. A visualização *Início* oferece estatísticas sobre seus hábitos de audição e relaciona suas faixas favoritas, mais recentes e menos reproduzidas. *Faixa Atual* apresenta dados relativos à faixa reproduzida no momento, como a capa

do disco data (consulte a “Gerenciador de capas” (p 123)), as estatísticas de audição referentes à faixa em questão e muito mais. Se você tiver interesse na letra da música, use a guia *Letra* para exibi-la.

Navegador de coleção

Use esta tela para gerenciar e exibir sua coleção pessoal de títulos. A tela da coleção pode incluir arquivos de vários locais. O ícone de chave inglesa da barra de ferramentas permite determinar os locais em que a busca de arquivos de música deve ser feita. Uma vez selecionados os diretórios, a busca começa automaticamente. O resultado é exibido em uma estrutura em árvore. Usando *Primário* e *Secundário*, organize as duas ramificações superiores da árvore de acordo com os critérios de *Álbum*, *Artista*, *Gênero* e *Ano*. Quando a visualização em forma de árvore estiver pronta, localize os títulos digitando-os no campo de entrada. A seleção feita na visualização o conduz até a primeira entrada correspondente à medida que você digita. Para atualizar os dados da sua coleção, inicie uma nova pesquisa do sistema de arquivos usando *Ferramentas → Pesquisar Coleção Novamente*.

Navegador de lista de reprodução

O navegador de lista de reprodução é dividido em duas partes. A parte superior relaciona todas as listas personalizadas criadas arrastando faixas para a janela da lista de reprodução e clicando em *Gravar Lista de Reprodução Como*. Para visualizar seu conteúdo, clique no sinal de + próximo ao nome da lista. Modifique essas listas arrastando e soltando. Para carregar uma delas, clique duas vezes na lista.

IMPORTANTE: Compartilhando listas de reprodução com outros leitores

Grave as listas de reprodução no formato `m3u` ou `pls` e compartilhe-as depois em outros leitores que usam esses formatos.

O amaroK pode compilar listas de reprodução úteis (“Listas de Reprodução Inteligentes”) dinamicamente. Use a parte inferior do navegador de lista de reprodução para selecionar uma das listas inteligentes ou clique em *Criar Lista de Reprodução Inteligente* para definir uma lista inteligente personalizada. Digite um nome, critério de pesquisa, ordem e limite de faixa opcional.

Navegador de Arquivos

Essa guia abre um navegador de arquivos. Ela corresponde à caixa de diálogo de seleção de arquivos do KDE padrão com os controles normais para navegar no sistema de arquivos. Digite um URL ou diretório diretamente no campo de entrada de texto. No conteúdo exibido, arraste elementos para a lista de reprodução para

incluí-los. Também é possível realizar uma pesquisa recursiva para encontrar um arquivo em um determinado diretório. Para fazer isso, digite uma string de texto para o título ou local onde a pesquisa será feita. Em seguida, selecione *Pesquisar* e aguarde os resultados serem exibidos na parte inferior da janela.

Gerenciador de capas

O amaroK vem com um gerenciador de capas que permite manter a correspondência entre os dados de música e imagem nos álbuns reproduzidos. Inicie o *Gerenciador de Capas* clicando em *Ferramentas → Gerenciador de Capas*. Uma visualização em forma de árvore no lado esquerdo da janela relaciona todos os álbuns da sua coleção. As capas recuperadas da Amazon são exibidas no lado direito da janela. Em *Visualização*, selecione o que deve ser exibido na visualização da lista de capas. *Todos os álbuns* lista a totalidade dos álbuns da sua coleção, independentemente de terem a imagem da capa ou não. *Álbuns com capa* relaciona somente os que possuem uma capa e *Álbuns sem capa* relaciona os que não têm capa. Para recuperar dados sobre capas, escolha seu *Local da Amazon* e depois clique em *Buscar Capas Ausentes*. O amaroK tenta obter as capas de todos os álbuns contidos na sua coleção.

Efeitos

Selecione o botão *FX* da janela do leitor ou use o menu do aplicativo amaroK para abrir uma caixa de diálogo na qual é possível ativar e configurar vários efeitos de som, como um equalizador, o equilíbrio de som estéreo e efeito surround. Selecione os efeitos desejados e ajuste as configurações, se disponíveis, para cada opção.

Visualizações

O amaroK é fornecido com inúmeras visualizações que exibem um efeito gráfico para a música reproduzida. As visualização nativas do amaroK são exibidas na janela do leitor. Veja os vários modos de exibição disponíveis clicando na animação.

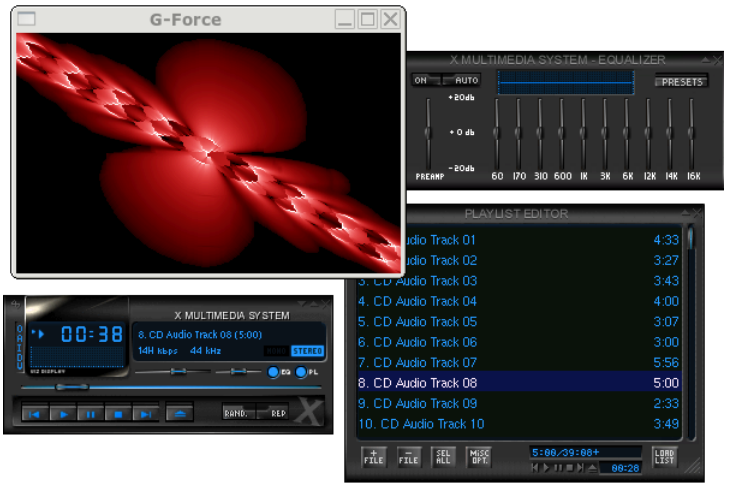
Além do acima descrito, o amaroK também dá suporte aos plug-ins de visualização do leitor de mídia XMMS. Para usá-los, primeiro instale o pacote `xmms-plugins` e selecione *Visualizações* no menu do amaroK. Será exibida a janela com os plug-ins disponíveis. Os plug-ins XMMS são sempre exibidos em outra janela. Em alguns casos, existe uma opção para exibi-los no modo de tela cheia. Com alguns plug-ins, talvez

você não consiga obter um efeito visual uniforme se não usar uma placa de vídeo de aceleração 3D.

7.2.2 XMMS

O XMMS é outro leitor de mídia com recursos completos e suporte avançado para áudio. Portanto, será muito rara a ocorrência de saltos e falhas durante a reprodução. O aplicativo é fácil de usar. O botão para exibir o menu está localizado no canto superior esquerdo da janela do programa. Para aqueles que preferirem uma aparência e funcionamento semelhante ao GNOME, está disponível uma versão GTK2 do XMMS, o Beep Media Player. Basta instalar o pacote `bmp`. Contudo, nem todos os plug-ins XMMS recebem suporte dessa porta de XMMS.

Figura 7.5 *O XMMS com Equalizer, OpenGL Spectrum Analyzer e Infinity Plug-Ins*


G-Force
X MULTIMEDIA SYSTEM - EQUALIZER
PRESETS
PREAMP
60 170 310 600 1K 3K 6K 12K 14K 16K
PLAYLIST EDITOR
1. CD Audio Track 01 4:33
2. CD Audio Track 02 3:27
3. CD Audio Track 03 3:43
4. CD Audio Track 04 4:00
5. CD Audio Track 05 3:07
6. CD Audio Track 06 3:00
7. CD Audio Track 07 5:56
8. CD Audio Track 08 5:00
9. CD Audio Track 09 2:33
10. CD Audio Track 10 3:49
X MULTIMEDIA SYSTEM
00:38
8. CD Audio Track 08 (5:00)
STEREO

Selecione o módulo de plug-in de saída com *Opções → Preferências → Plug-ins de E/S de Áudio*. Se o pacote `xmms-kde` estiver instalado, o servidor de som aRts poderá ser configurado aqui.

IMPORTANTE: Usando o plug-in de gravador de disco

O XMMS automaticamente redireciona sua saída para o *Plug-in de Gravador de Disco* se não conseguir encontrar uma placa de som configurada. Nesse

caso, os arquivos reproduzidos são gravados no disco rígido no formato WAV. O marcador de tempo é mais rápido na gravação do que na reprodução da saída executada por meio de uma placa de som.

Inicie os diversos plug-ins de visualização com *Opções → Preferências → Plug-Ins de Visualização*. Se você possui uma placa de vídeo com aceleração 3D, selecione um aplicativo como o analisador de espectro OpenGL. Se o pacote `xmms-plugins` estiver instalado, tente o plug-in Infinity.

À esquerda, abaixo do botão de menu, há cinco botões com letras diferentes. Esses botões permitem acesso rápido a menus, caixas de diálogo e configurações adicionais. Abra a lista de reprodução com *PL* e o equalizador com *EQ*.

7.3 CDs: Reprodução e ripagem

Existem muitas formas de reproduzir as faixas musicais de sua preferência. Você pode reproduzir um CD ou versões digitalizadas dos CDs. A seção abaixo apresenta alguns aplicativos de leitura de CDs, além de alguns aplicativos que podem ser usados para a ripagem e codificação de CDs de áudio.

IMPORTANTE: CDDA e reprodução analógica de CDs

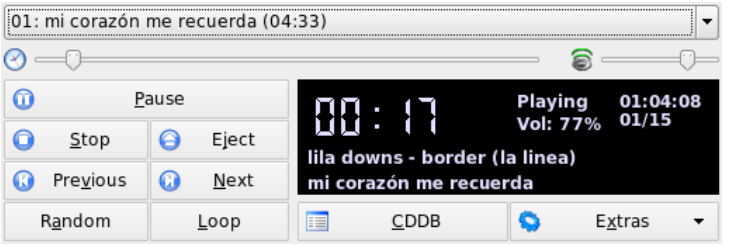
Há duas formas diferentes de reproduzir CDs de áudio. Unidades de CD e DVD capazes de realizar a reprodução analógica de CDs lêem os dados de áudio e os enviam ao dispositivo de saída de som. Algumas unidades externas conectadas via PCMCIA, FireWire ou USB precisam usar CDDA (Compact Disk Digital Audio) para primeiro extrair os dados de áudio e depois reproduzi-los como PCM digital. Os leitores apresentados nas seções a seguir não dão suporte ao CDDA. Use o XMMS se precisar de suporte ao CDDA.

7.3.1 KsCD — Leitor de CD de áudio

O KsCD é um leitor de CD de áudio fácil de usar. Ele é integrado na barra de tarefas do KDE e pode ser configurado para iniciar a reprodução automaticamente após a inserção de um CD. Para acessar o menu de configuração, selecione *Extras → Configurar KsCD*. Busque informações sobre álbuns e faixas de um servidor CDDB na Internet se o KsCD estiver configurado para isso. Você também pode fazer o upload

de informações de CDDB para fins de compartilhamento. Use a caixa de diálogo *CDDB* para a recuperação e upload de informações.

Figura 7.6 *Interface do usuário do KsCD*



7.3.2 Applet de reprodução de CD do GNOME

Este é um applet simples que pode ser integrado a um painel do GNOME. Com o ícone de ferramentas, configure seu comportamento e selecione um tema. Controle a reprodução com os botões situados na parte inferior da janela do leitor ou usando o menu de contexto que se abre ao clicar o botão direito do mouse no ícone do painel ou janela do leitor.

7.3.3 Compactando dados de áudio

A compactação de áudio pode ser feita por diversas ferramentas. As seções a seguir apresentam uma abordagem de linha de comando para a codificação e reprodução de dados de áudio, bem como alguns aplicativos gráficos capazes de realizar a compactação de áudio.

Ferramentas de linha de comando para a codificação e reprodução de dados de áudio

O Ogg Vorbis (pacote `vorbis-tools`) é um formato gratuito de compactação de áudio que hoje é suportado pela maioria dos leitores de áudio e até por leitores portáteis de MP3. O endereço da página do projeto é `http://www.xiph.org/ogg/vorbis`.

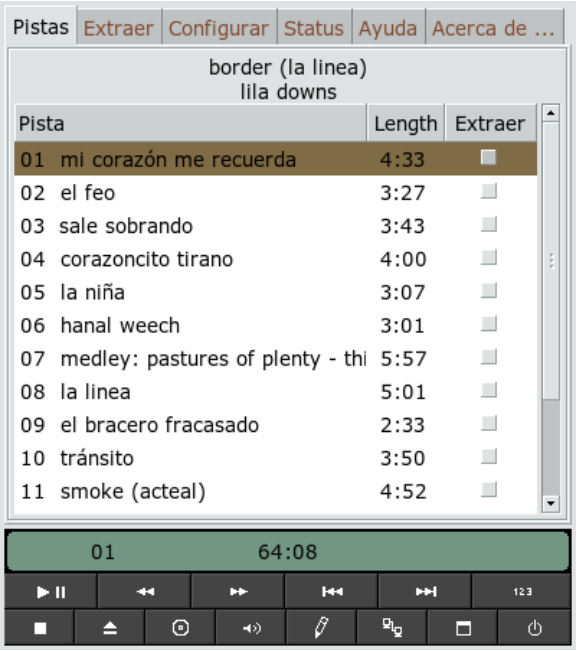
O SUSE Linux traz diversas ferramentas de suporte ao Ogg Vorbis. O `oggenc` é uma ferramenta de linha de comando para a codificação de arquivos WAV para o Ogg. Basta executar `oggenc` *`myfile.wav`* para transformar um determinado arquivo `.wav` em Ogg Vorbis. A opção `-h` exibe uma visão geral dos outros parâmetros. O Oggenc dá suporte à codificação com uma taxa de bits variável. Desse modo, um grau ainda maior de compactação pode ser alcançado. Em vez da taxa de bits, especifique a qualidade desejada com o parâmetro `-q`; já o parâmetro `-b` determine a taxa de bits média; `-m` e `-M` especificam a taxa de bits mínima e máxima.

O ogg123 é um leitor de linha de comando Ogg. Inicie-o com um comando como `ogg123` *`mysong.ogg`*.

Compactando dados de áudio usando o Grip

O Grip é um leitor e reprodutor de CDs do GNOME (veja a Figura 7.7, “Ripando CDs de áudio com o Grip” (p 128)). A funcionalidade de leitor de CD é totalmente controlada pelos botões situados na parte inferior da janela. Controle a funcionalidade de ripagem e codificação usando as guias localizadas na parte superior da janela. Para visualizar e editar as informações sobre faixa e álbum ou para selecionar as faixas para ripagem, abra a guia*Faixas*. Para selecionar uma faixa, clique na caixa de seleção próxima ao título da faixa. Para editar as informações sobre a faixa, clique em *Alternar editor de disco* e envie suas modificações. A guia *Ripar* seleciona o modo de ripagem de preferência e controla esse processo. Acesse a configuração inteira do Grip na guia *Config*. Use *Status* para verificar o status do aplicativo.

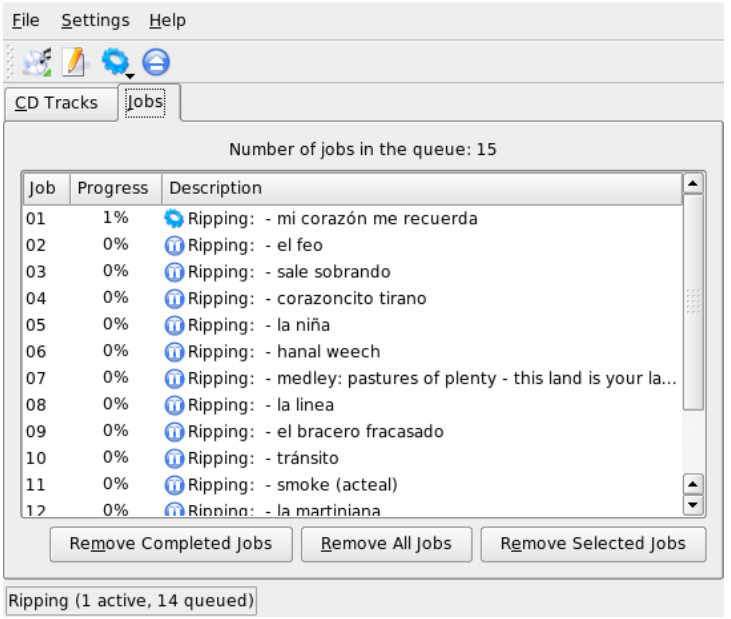
Figura 7.7 *Ripando CDs de áudio com o Grip*



Compactando dados de áudio usando o KAudioCreator

O KAudioCreator é um aplicativo simples de ripagem de CD (veja a Figura 7.8, "Ripando CDs de áudio com o KAudioCreator" (p 129)). Ao ser iniciado, ele lista todas as faixas do CD na guia *Faixas do CD*. Selecione as faixas para ripagem e codificação. Para editar as informações relativas a faixas, use o *Editor de Álbum* em *Arquivo → Editar Álbum*. Do contrário, basta iniciar a ripagem e codificação com *Arquivo → Ripar Seleção*. Observe o andamento dessas tarefas usando a guia *Tarefas*. Se configurado para tanto, o KAudioCreator também gera arquivos de lista de reprodução da sua seleção, que podem ser usados por leitores, como o amaroK e o XMMS.

Figura 7.8 *Ripando CDs de áudio com o KAudioCreator*

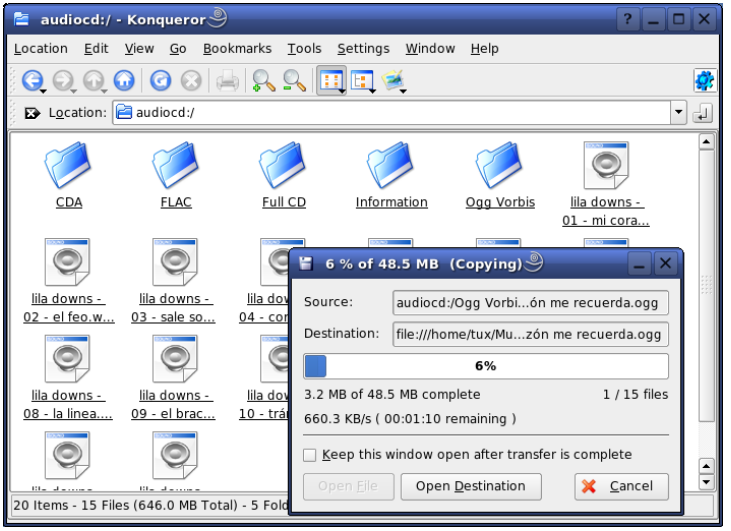

File Settings Help
CD Tracks
Jobs
Number of jobs in the queue: 15
Job Progress Description
01 1% Ripping: - mi corazón me recuerda
02 0% Ripping: - el feo
03 0% Ripping: - sale sobrando
04 0% Ripping: - corazoncito tirano
05 0% Ripping: - la niña
06 0% Ripping: - hanal weech
07 0% Ripping: - medley: pastures of plenty - this land is your la...
08 0% Ripping: - la linea
09 0% Ripping: - el bracero fracasado
10 0% Ripping: - tránsito
11 0% Ripping: - smoke (acteal)
Remove Completed Jobs
Remove All Jobs
Remove Selected Jobs
Ripping (1 active, 14 queued)

Compactando CDs de áudio usando o Konqueror

Antes de iniciar o processo de ripagem propriamente dito com o Konqueror, configure o tratamento de CDs de áudio e o codificador Ogg Vorbis no Centro de Controle KDE. Selecione *Som & Multimídia → CDs de Áudio*. O módulo de configuração é dividido em três guias: *Geral*, *Nomes* e *Codificador Ogg Vorbis*. Normalmente, um dispositivo de CD adequado é detectado automaticamente. Não mude esse padrão, a menos que a detecção automática tenha falhado e você precise ajustar o dispositivo de CD manualmente. A correção de erros e a prioridade do codificador também podem ser definidas aqui. A guia *Codificador Ogg Vorbis* determina a qualidade da codificação. Para configurar a busca online de informações sobre álbuns, faixas e artistas para a sua ripagem de dados de áudio, selecione *Adicionar Informações sobre Faixa*.

Para iniciar o processo de ripagem, insira o CD na unidade de CD-ROM e digite `audiocd:/` na barra *Local*. Em seguida, o Konqueror relaciona as faixas do CD e algumas pastas (veja a Figura 7.9, “Ripando dados de áudio com o Konqueror” (p 130)).

Figura 7.9 *Ripando dados de áudio com o Konqueror*

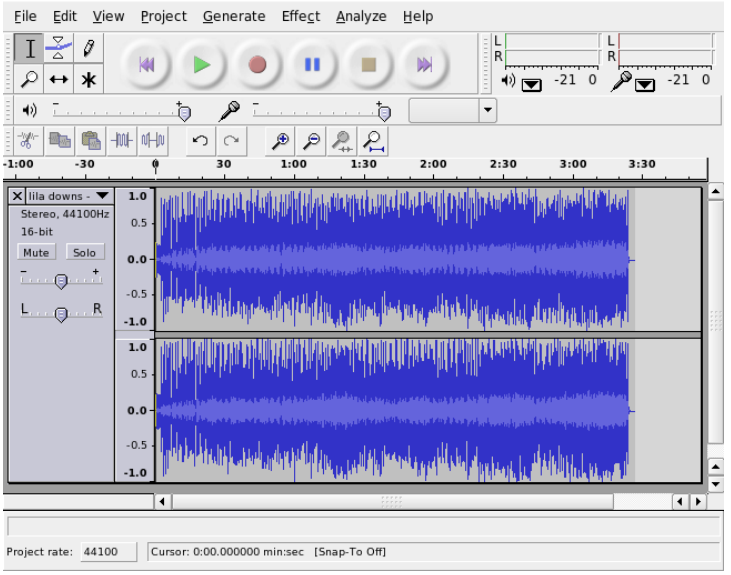

audiocd:/ - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: audiocd:/
CDA
FLAC
Full CD
Information
Ogg Vorbis
lila downs - 01 - mi cora...
lila downs - 02 - el feo.w...
lila downs - 03 - sale so...
lila downs - 08 - la linea....
lila downs - 09 - el brac...
6 % of 48.5 MB (Copying)
Source: audiocd:/Ogg Vorbi...ón me recuerda.ogg
Destination: file:///home/tux/Mu...zón me recuerda.ogg
6%
3.2 MB of 48.5 MB complete
1 / 15 files
660.3 KB/s (00:01:10 remaining)
Keep this window open after transfer is complete
Open File
Open Destination
Cancel
20 Items - 15 Files (646.0 MB Total) - 5 Fold

Para manter dados de áudio descompactados no disco, basta selecionar os arquivos `.wav` e arrastá-los até outra janela do Konqueror para copiá-los para o destino final. Para iniciar a codificação do Ogg Vorbis, arraste a pasta `Ogg Vorbis` para outra janela do Konqueror. A codificação começa logo que você solta a pasta Ogg Vorbis em seu destino.

7.4 Gravação no disco rígido com o Audacity

O audacity (pacote `audacity`) grava e edita arquivos de áudio. Esse processo é chamado de gravação no disco rígido. Ao iniciar o programa pela primeira vez, selecione o idioma. Nas outras ocasiões, mude a configuração de idioma em *Arquivo* → *Preferências* → *Interface*. A mudança de idioma passa a valer na próxima vez que o programa for iniciado.

Figura 7.10 *Visualização espectral dos dados de áudio*


File Edit View Project Generate Effect Analyze Help
-1:00 -30 0 30 1:00 1:30 2:00 2:30 3:00 3:30
lila downs -
Stereo, 44100Hz
16-bit
Mute Solo
L R
1.0 0.5 0.0 -0.5 -1.0
Project rate: 44100
Cursor: 0:00.000000 min:sec [Snap-To Off]

7.4.1 Gravando arquivos WAV e importando arquivos

Clique no botão vermelho de gravação para criar um faixa estéreo vazia e iniciar a gravação. Para mudar os parâmetros padrão, defina as configurações desejadas em *Arquivo → Preferências*. *E/S de Áudio* e *Qualidade* são importantes para a gravação. Mesmo que já existam faixas, ao pressionar o botão de gravação novas faixas são criadas. Esse processo pode ser confuso a princípio, pois essas faixas não podem ser vistas na janela do programa de tamanho padrão.

Para importar arquivos de áudio, selecione *Projeto → Importar Áudio*. O programa dá suporte ao formato WAV e ao formato Ogg Vorbis compactado. Consulte a Seção 7.3.3, "Compactando dados de áudio" (p 126) para obter mais informações sobre esse formato.

7.4.2 Editando arquivos de áudio

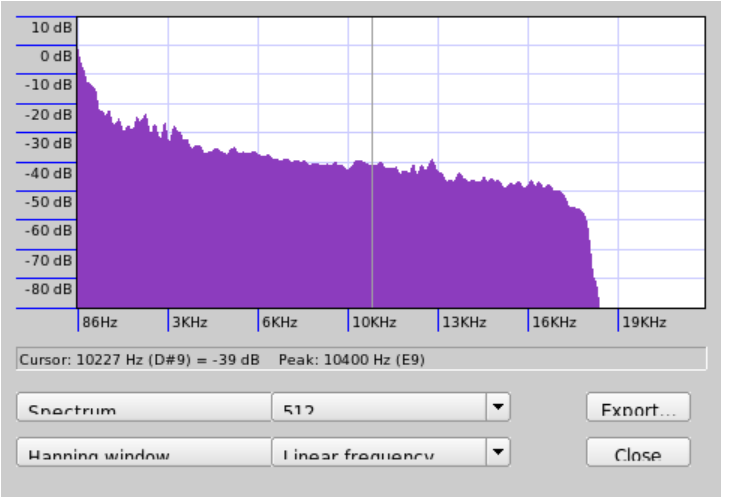
Abra o menu *AudioTrack* no lado esquerdo da faixa. Esse menu oferece diversas opções de diferentes visualizações e operações básicas de edição. Para renomear a faixa, selecione *Nome* e digite o novo nome. Os diferentes modos de visualização oferecidos pelo Audacity incluem *Waveform*, *Waveform (dB)*, *Spectrum* e *Pitch*. Escolha aquele que atender às suas necessidades. Caso deseje editar cada canal de uma faixa estéreo separadamente, selecione *Dividir Faixa*. Em seguida, cada canal pode ser tratado como uma faixa separada. Defina *Formato de Amostra* (em bits) e *Taxa de Amostra* (em Hz) para cada faixa.

Antes de usar a maioria das ferramentas oferecidas no menu *Editar*, primeiro selecione o canal e o segmento da faixa a editar. Após fazer a seleção, você pode aplicar todo tipo de modificação e efeitos a ela.

Dependendo do tipo de arquivo escolhido, diversos formatos de visualização para seleções de segmentos são oferecidos em *Visualização → Definir Formato da Seleção*. Com o recurso *Ajustar ao Modo*, os limites do segmento podem ser automaticamente ajustados ao formato de visualização selecionados. Por exemplo, se você selecionar *Frames PAL* como o formato de visualização e ativar *Instantâneo*, os limites de segmentos serão sempre selecionados em múltiplos de frames.

Como todas as ferramentas de edição vêm com dicas, seu uso fica fácil. A função *Histórico de Desfazer*, acessada em *Visualização → Histórico*, é um útil recurso para exibir etapas de edição recentes e desfazê-las clicando na lista. Use a função *Descartar* com cautela, pois ela apaga etapas de edição da lista. Uma vez descartadas, essas etapas não podem mais ser desfeitas.

Figura 7.11 *Espectro*



O analisador de espectro interno assiste na rápida identificação de ruídos. Para visualizar o espectro do segmento selecionado, vá até *Visualização → Plotar Espectro*. Selecione uma escala de freqüência logarítmica em oitavos com *Freqüência Logarítmica*. Quando você move o ponteiro do mouse no interior do espectro, as freqüências dos picos são automaticamente exibidas juntas com as respectivas notas.

Para remover freqüências indesejadas, vá até *Efeito → Filtro FFT*. Em conexão com o processo de filtragem, pode ser necessário reajustar a amplitude do sinal com *Amplificar*. Além disso, use *Amplificar* para verificar a amplitude. Por padrão, a *Amplitude de Novos Picos* é definida em 0.0 dB. Esse valor representa a amplitude máxima no formato de áudio selecionado. *Amplificação* mostra o valor necessário para amplificar o segmento selecionado até a amplitude desse pico. Um valor negativo indica excesso de amplificação.

7.4.3 Gravando e exportando

Para gravar o projeto inteiro, selecione *Arquivo → Gravar Projeto* ou *Gravar Projeto Como*. Essa ação gera um arquivo XML com a extensão `.aup`, que descreve o projeto. Os dados de áudio efetivos são gravados em um diretório com o mesmo nome do projeto com a extensão `_data`.

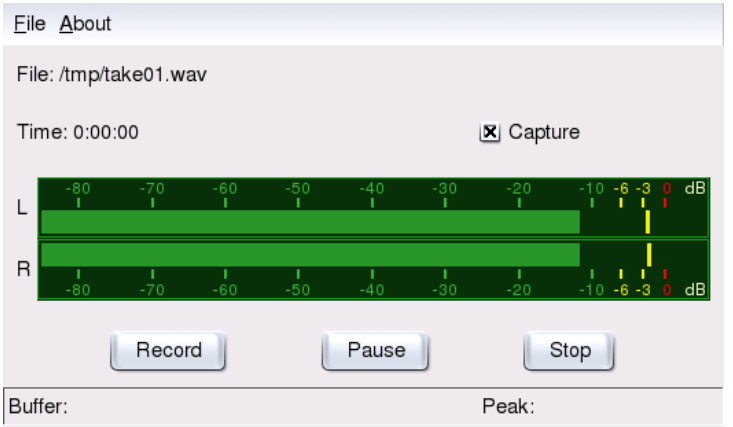
O projeto inteiro ou o segmento selecionado atualmente também pode ser exportado como um arquivo WAV estéreo. Para exportar o projeto em formato Ogg Vorbis, consulte as informações contidas na Seção 7.3.3, “Compactando dados de áudio” (p 126).

7.5 Gravação direta e reprodução de arquivos WAV

Os programas `arecord` e `aplay`, contidos no pacote `alsa`, oferecem uma interface simples e flexível com os dispositivos PCM. Já os programas `arecord` e `aplay` podem ser usados para gravar e reproduzir dados de áudio em vários formatos, inclusive WAV. O comando `arecord -d 10 -f cd -t wav mysong.wav` grava um arquivo WAV de 10 segundos em qualidade de CD (16 bit, 44,1 kHz). Para listar todas as opções do `arecord` e `aplay`, execute-os com a opção `--help`.

O qaRecord (pacote `kalsatools`) é um programa de gravação simples com uma interface gráfica e exibição de nível. Tendo em vista que esse programa usa um buffer interno de aproximadamente 1 MB (configurável com `--buffersize`), ele permite gravações ininterruptas mesmo em hardware lento, sobretudo se for executado com prioridade de tempo real. Durante a gravação, o tamanho do buffer em uso é exibido na linha de status em *Buffer* e o tamanho máximo do buffer necessário até o momento para essa gravação é exibido em *Pico*.

Figura 7.12 *QARecord — Um aplicativo de gravação de disco rígido simples*



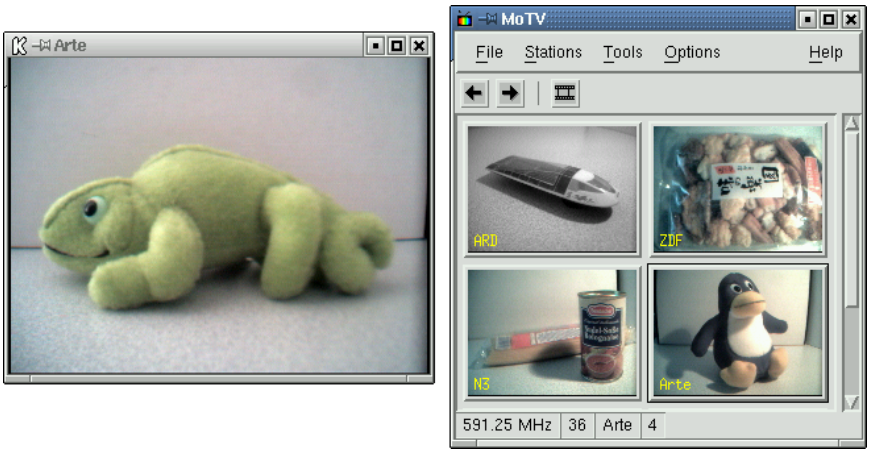
8 TV, vídeo, rádio e webcam

Este capítulo apresenta alguns aplicativos básicos de vídeo, rádio e webcam do Linux. Aprenda a configurar e usar o motv para assistir TV analógica, usar uma webcam e navegar pelo texto do vídeo. Use o xawtv4 para transmissões digitais de vídeo. As webcams podem ser executadas com o uso do gqcam. Informações sobre o EPG podem ser acessadas com o uso do nxtvepg ou do xawtv4.

8.1 Assistindo TV com o motv

O motv é um sucessor aperfeiçoado do xawtv. Ele incorpora todas as funções essenciais à interface do usuário. Inicie o aplicativo com *Multimídia → Vídeo → motv*. Inicie-o na linha de comando com `motv`. Inicialmente, apenas uma janela de TV aparece depois que o aplicativo é iniciado. Clique o botão direito do mouse em uma janela de menu para abri-la.

Figura 8.1 *Aplicativo de TV motv*



8.1.1 Fonte de vídeo e pesquisa de rede

Em *Configurações → Entrada*, selecione a fonte de vídeo. Se você selecionar *Televisão* aqui, configure a rede de transmissão antes de iniciar o aplicativo. Isso ocorre automaticamente com a pesquisa de rede, também localizada no menu *Configurações*. Se você clicar em *Gravar configurações*, a rede encontrada será inserida no arquivo `.xawtv` do seu diretório pessoal e estará disponível na próxima vez em que o aplicativo for iniciado.

DICA: Selecionando canais

Se você não quiser percorrer todos os canais disponíveis, localize o próximo canal com Ctrl + ↑. Se necessário, ajuste também a freqüência de transmissão com ← ou →.

8.1.2 Recuperando dados de áudio

A saída de áudio da placa de TV é conectada à entrada de linha da sua placa de som, aos alto-falantes ou a um amplificador. Algumas placas de TV podem mudar o volume da saída de áudio. O volume pode ser configurado com os controles deslizantes exibidos

depois que você seleciona *Configurações → Barra Deslizante*. Essa janela também contém os controles deslizantes que definem brilho, contraste e cor.

Para usar sua placa de som para reprodução de áudio, verifique as configurações do mixer usando o gamix, descritas na Seção 7.1, “Mixers” (p 115). Para placas de som que atendem às especificações AC97, defina *Entrada-MUX* como *Linha*. O volume pode ser posteriormente ajustado com os controles deslizantes *Master* e *Linha*.

8.1.3 Proporções de tela e modo de tela cheia

A maioria das imagens de televisão tem uma proporção de altura e largura de 4:3. Essas proporções podem ser definidas em *Ferramentas → Dimensões de Tela*. Se *4:3* for selecionado (esta é a configuração padrão), as dimensões de tela serão mantidas automaticamente, mesmo quando o tamanho da tela for alterado.

Com F ou *Ferramentas → Tela cheia*, mude para o modo de tela cheia. Se a imagem de TC no modo de tela cheia não se dimensionar no monitor inteiro, será necessário realizar um ajuste manual. Muitas placas de vídeo podem dimensionar a imagem de televisão do modo de tela cheia no tamanho total do monitor sem alterar o modo de vídeo. Se sua placa não suporta essa função, o modo de vídeo deve ser alterado para 640x480 para o modo de tela cheia. Crie a configuração relacionada em *Configurações → Configuração*. Depois de reiniciar o motv, o modo de monitor também será alterado se você tiver mudado para o modo de tela cheia.

DICA: Armazenando a configuração no .xawtv

Para que o arquivo `.xawtv` seja criado automaticamente e atualizado, clique em *Configurações → Gravar configurações*. Os transmissores serão gravados com a configuração. Para obter mais informações sobre o arquivo de configuração, consulte a página do manual sobre o `xawtvrc`.

8.1.4 Menu disparador

Use o menu Disparador para iniciar outros aplicativos e usá-los com o motv. Inicie o mixer de áudio gamix e o aplicativo de texto de vídeo alevt, por exemplo, usando um

atalho de teclado. Os aplicativos a serem iniciados a partir do motv devem ser inseridos no arquivo `.xawtv`. As entradas devem ser como:

```
[launch] Gamix = Ctrl+G, gamix AleVT = Ctrl+A, alevt
```

O atalho e o comando usados para iniciar o aplicativo devem concordar com o nome do aplicativo propriamente dito. Inicie os aplicativos especificados em [launch] por meio do menu *Ferramenta*.

8.2 Suporte ao texto de vídeo

Use alevt para navegar em páginas de texto de vídeo. Inicie o aplicativo com *Multimídia → Vídeo → alevt* ou na linha de comando com `alevt`.

O aplicativo grava todas as páginas da estação selecionada ativadas com o motv. Navegue pelas páginas digitando o número de página desejado ou clicando no número de página. Avance ou volte páginas clicando em << ou >>, localizado na margem da janela inferior.

Versões recentes do motv e de seu sucessor, o xawtv4, incluem seus próprios aplicativos viewers de texto de vídeo: mtt (motv) e mtt4 (xawtv4). O mtt4 suporta até mesmo placas DVB.

8.3 Webcams e motv

Se sua webcam já é suportada pelo Linux, acesse-a com o motv. Encontre um resumo dos dispositivos USB suportados em `http://www.linux-usb.org`. Se você já tiver usado o motv para acessar a placa de TV antes de acessar a webcam, o driver do bttv já estará carregado. O driver da webcam é carregada automaticamente quando a webcam é conectada à USB. Inicie o motv na linha de comando com o parâmetro `-c /dev/video1` para acessar a webcam. Acesse a placa de TV com `motv -c /dev/video0`.

Quando você conecta a webcam à porta USB antes de o driver bttv ser automaticamente carregado (por exemplo, iniciando um aplicativo de TV), `/dev/video0` é reservado para a webcam. Neste caso, se você iniciar o motv com o parâmetro `-c /dev/video1` para acessar a placa de TV, poderá receber uma mensagem de erro, porque o driver do bttv não foi automaticamente carregado. Solucione esse problema carregando o driver

separadamente com `modprobe bttv` como usuário `root`. Acesse uma visão geral dos dispositivos de vídeo configuráveis no sistema com `motv -hwscan`.

8.4 nxtvepg – Revista de TV para seu PC

Em algumas estações emissoras, é transmitido um sinal EPG (Electronic Program Guide, Guia Eletrônico de Programação) com o sinal de texto de vídeo. Visualize esse guia eletrônico facilmente usando o programa nxtvepg. Para isso, no entanto, é necessário ter uma placa de TV suportada pelo driver bttv e ser capaz de receber algum dos canais transmitidos com EPG.

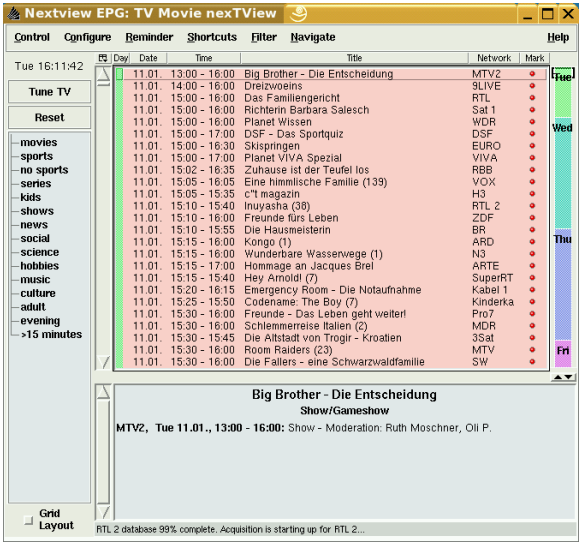
Com o nxtvepg, as transmissões são classificadas por canal e tópico, como *cinema* e *esporte*, e filtradas segundo critérios como *Ao Vivo*, *Estéreo* ou *Legendado*. Inicie o aplicativo com *Multimídia → Vídeo → nxtvepg* ou na linha de comando, com `nxtvepg`.

8.4.1 Importando o banco de dados do EPG

Para configurar e atualizar o banco de dados de programação usando o sinal EPG, ajuste o sintonizador da placa de TV na estação que transmite o EPG. Isso pode ser feito com um aplicativo de TV, como motv ou nxtvepg. Apenas um aplicativo pode acessar o sintonizador por vez.

Se você definir um transmissor de EPG no motv, o nxtvepg começará imediatamente a importar a lista atual de programação da TV. O andamento da importação será exibido.

Figura 8.2 *Revista eletrônica de TV nxtvepg*


Nextview EPG: TV Movie nexTView
Control Configure Reminder Shortcuts Filter Navigate Help
Tue 16:11:42
Tune TV
Reset
movies
sports
no sports
series
kids
shows
news
social
science
hobbies
music
culture
adult
evening
>15 minutes
Grid
Layout
Day Date Time Title Network Mark
11.01. 13:00 - 16:00 Big Brother - Die Entscheidung MTV2
11.01. 14:00 - 16:00 Dreizwoeins 9LIVE
11.01. 15:00 - 16:00 Das Familiengericht RTL
11.01. 15:00 - 16:00 Richterin Barbara Salesch Sat.1
11.01. 15:00 - 16:00 Planet Wissen WDR
11.01. 15:00 - 17:00 DSF - Das Sportquiz DSF
11.01. 15:00 - 16:30 Skispringen EURO
11.01. 15:00 - 17:00 Planet VIVA Spezial VIVA
11.01. 15:02 - 16:35 Zuhause ist der Teufel los RBB
11.01. 15:05 - 16:05 Eine himmlische Familie (139) VOX
11.01. 15:05 - 15:35 c't magazin H3
11.01. 15:10 - 15:40 Inuyasha (38) RTL 2
11.01. 15:10 - 16:00 Freunde fürs Leben ZDF
11.01. 15:10 - 15:55 Die Hausmeisterin BR
11.01. 15:15 - 16:00 Kongo (1) ARD
11.01. 15:15 - 16:00 Wunderbare Wasserwege (1) N3
11.01. 15:15 - 17:00 Hommage an Jacques Brel ARTE
11.01. 15:15 - 15:40 Hey Arnold! (7) SuperRT
11.01. 15:20 - 16:15 Emergency Room - Die Notaufnahme Kabel 1
11.01. 15:25 - 15:50 Codename: The Boy (7) Kinderka
11.01. 15:30 - 16:00 Freunde - Das Leben geht weiter! Pro7
11.01. 15:30 - 16:00 Schlemmerreise Italien (2) MDR
11.01. 15:30 - 15:45 Die Altstadt von Trogir - Kroatien 3Sat
11.01. 15:30 - 16:00 Room Raiders (23) MTV
11.01. 15:30 - 16:00 Die Fallers - eine Schwarzwaldfamilie SW
Tue
Wed
Thu
Fri
Big Brother - Die Entscheidung
Show/Gameshow
MTV2, Tue 11.01., 13:00 - 16:00: Show - Moderation: Ruth Moschner, Oli P.
RTL 2 database 99% complete. Acquisition is starting up for RTL 2...

Se você não tiver iniciado um aplicativo de TV, o nxtvepg poderá procurar transmissores de EPG. Para isso, use *Configurar → Pesquisar provedores*. *Use .xatv* é ativado por padrão. Isso indica que o nxtvepg está acessando os transmissores gravados nesse arquivo.

DICA: Solução de problemas

Se houver problemas, verifique se a fonte de vídeo adequada foi escolhida em *Entrada de placa de TV*.

Selecione um dos provedores de EPG encontrados em *Configurar → Selecionar Provedor*. *Configurar → Mesclar Provedores* cria até mesmo associações flexíveis entre os vários bancos de dados de provedores.

8.4.2 Classificando os programas

O nxtvepg fornece uma função de filtragem conveniente para o gerenciamento até mesmo das mais amplas ofertas de programação. Ative uma lista de seleção de rede com *Configurar → Mostrar redes*. O menu *Filtrar* oferece várias funções de filtragem.

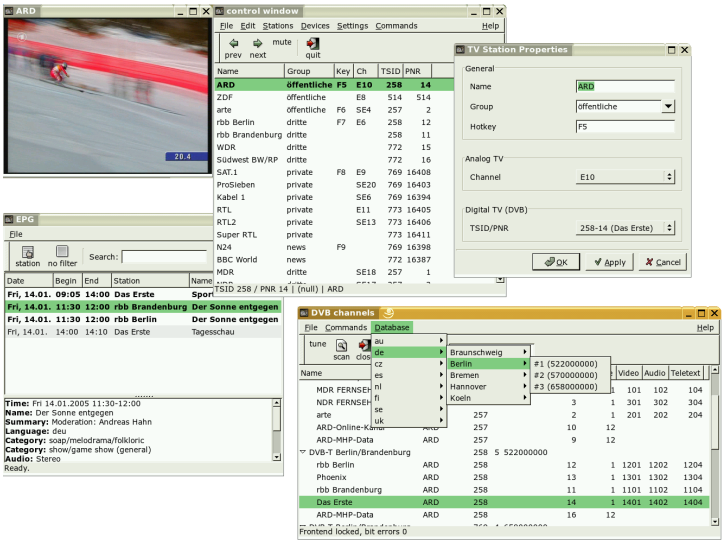
Clique o botão direito do mouse na lista de programas para abrir um menu de filtragem especial e ativar funções de filtragem contextual.

O menu *Navegar* é especialmente interessante. Ele é criado diretamente com dados do EPG. O menu aparece no idioma usado pela rede.

8.5 Assistindo transmissões de vídeo digital com o xawtv4

Depois que o hardware tiver sido configurado adequadamente com o YaST, inicie o xawtv4 a partir do menu principal (*Multimídia → Vídeo → xawtv4*). Para que você possa realmente começar a assistir suas transmissões favoritas, crie um banco de dados de estações do DVB.

Figura 8.3 *Executando o xawtv4*



Clique o botão direito do mouse na janela inicial para abrir a janela de controle (consulte a Figura 8.3, “Executando o xawtv4” (p 141)). Comece a exploração das estações do DVB disponíveis com *Editar → Explorar DVB*. É aberta uma janela de scanner de canal e browser. Selecione um conjunto para preparar a exploração. Isso pode ser feito manualmente com *Comandos → Ajustar manualmente*, se você já souber os parâmetros

de ajuste do conjunto, ou solicitando esses parâmetros de um banco de dados interno do xawtv4 via *Banco de Dados → _país_ → _número-do-canal_* (substitua *_país_* e *_número-do-canal_*) pelos valores reais para sua localização.

Assim que o scanner for ajustado, os primeiros dados serão exibidos na janela do browser. Inicie uma exploração completa de todas as estações disponíveis com *Comando → Pesquisa Completa*. Enquanto o scanner estiver em execução, você pode selecionar suas estações favoritas e adicioná-las à lista de estações simplesmente arrastando-as para a janela de controle. Saia do scanner de canal e selecione um dos canais para começar a assistir a transmissão.

DICA: Editando a lista de estações

Usando atalhos de teclado, controle a seleção dos canais com o teclado. Para definir um atalho para qualquer estação de sua lista, selecione a estação, clique em *Editar → Editar Estação*. Uma caixa de diálogo chamada *Propriedades da Estação de TV* é aberta. Insira o atalho e saia da caixa de diálogo com *OK*. Essa caixa de diálogo também permite definir submenus com grupos de estações (como “notícias” ou “particulares”).

O pacote de software do xawtv4 contém vários aplicativos multimídia independentes úteis:

pia4
: Um aplicativo reprodutor de filmes controlado apenas por linha de comando que pode ser usado para reproduzir qualquer fluxo de filme gravado pelo xawtv4.

mtt4
: Um browser de texto de vídeo (consulte a Figura 8.4, “O browser de texto de vídeo mtt4” (p 143)).

Figura 8.4 *O browser de texto de vídeo mtt4*

teletext: ARD
File Edit Go to Region Subpage Station Font Help
index prev next close
100 719 ARDtext Mo 17.01.05 15:32:11
Der Videotext
im Ersten
Index
> 101
US-Reporter: USA spähen Iran aus. 120
Mehr als 175.000 Tsunami-Opfer... 122
Reform des EU-Stabilitätspakts?.. 123
Kobe: Gedenken an Erdbebenopfer.. 530
Tennis: Schüttler und Haas weiter 204
Fußball: Allstar-Team gewählt.... 216
Handball:Brandt nominiert WM-Team 220
15.15 Abenteuer Wildnis..... 317
Kinder des Dschungels
16.00 Fliege - Die Talkshow. 318
Tagesschau 110/112 Kultur 500
Wetter ..... 170 Gesellschaft 530
Sport .... 200/600 Lotto/Toto .. 666
Das Erste 300/400 Wirtschaft .. 700
Internet: www.ard-text.de
Übersicht Inhalt > tagesschau >>

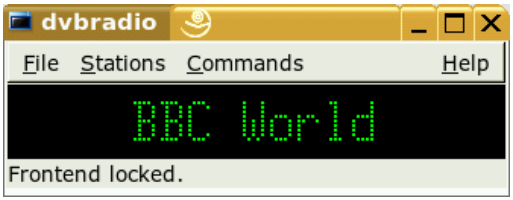
alexplore

Um aplicativo scanner de canal DVB independente. Sua funcionalidade é integrada ao xawtv4.

dvbradio

Um reprodutor de rádio DVB. Use-o para ouvir fluxos de rádio DVB-S após ter concluído a exploração inicial de estações (consulte a Figura 8.5, “Rádio DVB” (p 143)).

Figura 8.5 *Rádio DVB*



dvbrowse

Um aplicativo de browser de EPG. Use-o para obter informações de EPG após ter concluído a exploração inicial de estações.

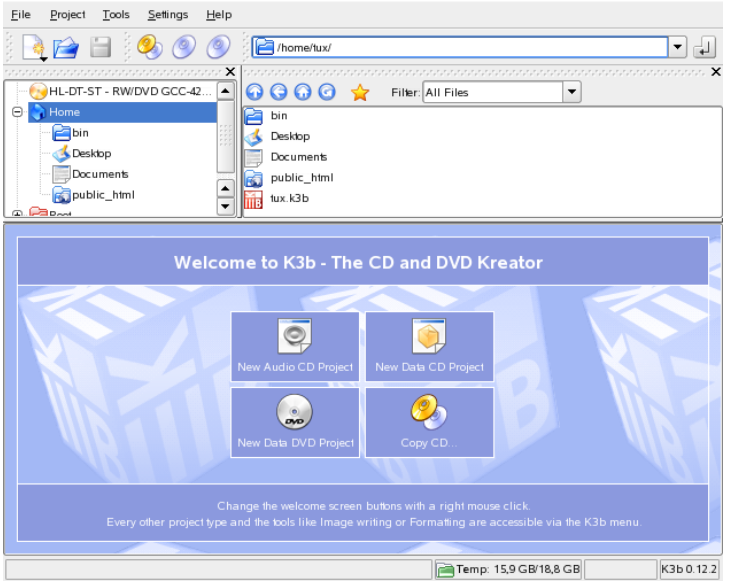
9 K3b — Gravando CDs ou DVDs

O K3b é um programa abrangente para a gravação de CDs e DVDs de dados e de áudio. Inicie o programa no menu principal ou digitando o comando `k3b`. As seções a seguir oferecem a você um resumo de como iniciar um processo de gravação básico para obter o seu primeiro CD ou DVD feito no Linux.

9.1 Criando um CD de dados

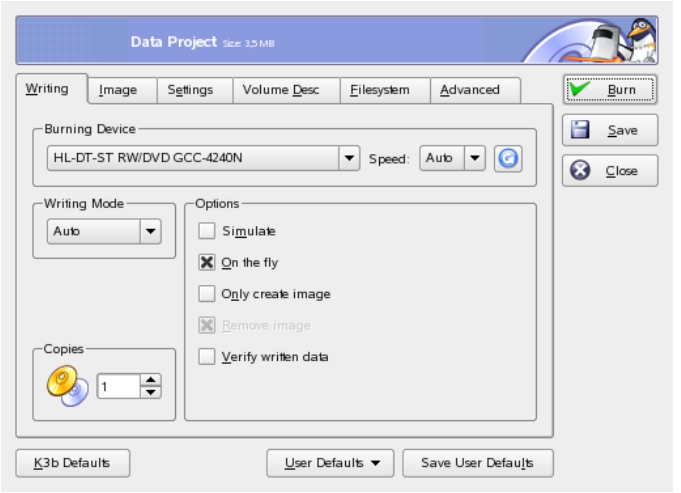
Para criar um CD de dados, vá para *Arquivo* → *Novo Projeto* → *Novo Projeto de Dados*. A tela do projeto é exibida na parte inferior da janela, como mostrado na Figura 9.1, “Criando um novo CD de dados” (p 146). Arraste os diretórios ou arquivos individuais desejados do diretório principal para a pasta do projeto e solte-os. Nomeie e grave o projeto usando *Arquivo* → *Gravar como*.

Figura 9.1 *Criando um novo CD de dados*



Selecione *Queimar* na barra de ferramentas ou pressione Ctrl + B. Será exibida uma caixa de diálogo com seis guias que oferecem várias opções para a gravação do CD. Consulte a Figura 9.2, “Personalizando o processo de gravação” (p 147).

Figura 9.2 *Personalizando o processo de gravação*



A guia *Gravando* possui várias configurações para o dispositivo de gravação, como opções de velocidade e gravação. Estas são as opções oferecidas:

Dispositivo de Gravação

O gravador detectado é exibido neste menu popup. Você pode selecionar a velocidade aqui também.

ATENÇÃO: Tenha cuidado ao selecionar a velocidade de gravação

Normalmente, você deve selecionar *Automático*, que opta pela velocidade máxima de gravação possível. No entanto, se você aumentar esse valor, mas o seu sistema não for capaz de enviar os dados de modo rápido o suficiente, a probabilidade de que ocorra um esvaziamento do buffer aumentará.

Modo de Gravação

Esta opção determina como o laser gravará o CD. No modo DAO (disk at once), o laser não é desativado enquanto o CD está sendo gravado. Esse modo é recomendado para a criação de CDs de áudio. No entanto, nem todos os CDs podem usá-lo. No modo TAO (track at once), um processo de gravação separado é usado para cada trilha individual. O modo RAW não é usado com freqüência, pois o gravador não corrige os dados. A melhor configuração é a do modo *Automático*, pois permite ao K3b usar as configurações mais adequadas.

Simular

Esta função pode ser usada para verificar se seu sistema suporta a velocidade de gravação escolhida. A gravação é realizada com o laser desativado para testar o sistema.

On the Fly

Grava os dados desejados sem primeiro criar um arquivo de imagem (não use esse recurso em máquinas de baixo desempenho). Um arquivo de imagem, também conhecido como imagem ISO, é um arquivo que armazena o conteúdo inteiro do CD e que, posteriormente, é gravado como está.

Somente Criar Imagem

Esta opção cria um arquivo de imagem. Defina o caminho desse arquivo em *Arquivo Temporário*. O arquivo de imagem pode ser gravado em CD posteriormente. Para isso, use *Ferramentas → CD → Queimar Imagem de CD*. Se essa opção for usada, todas as outras opções dessa seção serão desativadas.

Remover Imagem

Remova o arquivo de imagem temporário do disco rígido ao concluir.

Verificar Dados Gravados

Verifique a integridade dos dados gravados, comparando as somas do MD5 dos dados originais e dos gravados.

A guia *Imagem* só pode ser acessada se a opção *Somente criar imagem* da guia anterior estiver selecionada. Se esse for o caso, você pode determinar o arquivo em que o ISO será gravado.

A guia *Configurações* contém duas opções: *Modo de Trilha de Dados* e *Multissessão*. As opções do *Modo de Trilha de Dados* contêm a configuração de como as trilhas de dados podem ser gravadas. Em geral, *Automático* é considerado o método mais adequado. O *Multissessão* é usado para acrescentar dados a um CD já gravado, mas que ainda não foi finalizado.

Na guia *Descrição do Volume*, digite algumas informações gerais que podem ser usadas para identificar esse projeto de dados específico, seu editor e elaborador, bem como o aplicativo e sistema operacional usados em sua criação.

Em *Sistema de Arquivo*, especifique configurações para o sistema de arquivos do CD (RockRidge, Joliet, UDF). Determine, também, como serão tratados links simbólicos,

permissões de arquivos e espaços em branco. Na guia *Avançado*, usuários experientes podem criar outras configurações.

Após ajustar todas as configurações necessárias, inicie realmente o processo de gravação usando *Queimar*. Uma outra opção é gravar essas configurações para uso e ajuste futuros com *Salvar*.

9.2 Criando um CD de áudio

Basicamente não há diferenças significativas entre a criação de um CD de áudio e de um CD de dados. Selecione *Arquivo → Novo Projeto de Áudio*. Arraste cada trilha de áudio e solte-a na pasta do projeto. Os dados de áudio devem estar no formato WAV ou Ogg Vorbis. Determine a seqüência das trilhas movendo-as para cima ou para baixo na pasta do projeto.

Com a ajuda de CD-Texto, você pode adicionar determinadas informações de texto a um CD, como o título do CD, o nome do artista e da trilha. Leitores de CD que suportam esse recurso podem ler e exibir essas informações. Para adicionar informações de CD-Texto às suas trilhas de áudio, selecione primeiro a trilha. Clique com o botão direito do mouse e selecione *Propriedades*. Será aberta uma nova janela para que você digite suas informações.

A caixa de diálogo de gravação do CD de áudio não é muito diferente da exibida na gravação do CD de dados. No entanto, os modos *Disco imediatamente* e *Trilha imediatamente* são de maior importância. O modo *Trilha imediatamente* insere um intervalo de dois segundos após cada trilha.

DICA: Preservando a integridade dos dados

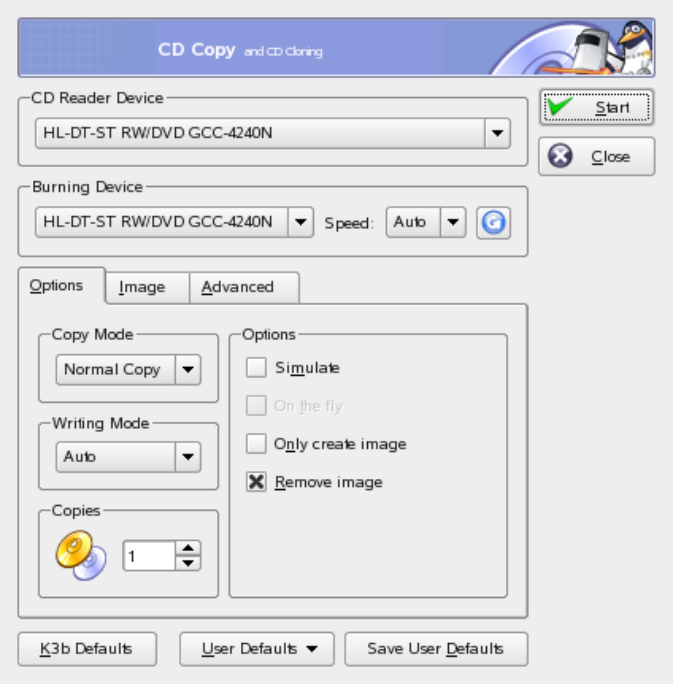
Ao gravar CDs de áudio, escolha uma velocidade de gravação menor para reduzir o risco de erros de gravação.

Após ajustar todas as configurações necessárias, inicie realmente o processo de gravação usando *Queimar*. Uma outra opção é gravar essas configurações para uso e ajuste futuros com *Salvar*.

9.3 Copiando um CD ou DVD

Selecione *Ferramentas → Copiar CD* ou *Ferramentas → Copiar DVD*, dependendo da mídia. Na caixa de diálogo que é aberta, configure o dispositivo de leitura e gravação como mostrado na Figura 9.3, “Copiando um CD” (p 150). As opções de gravação discutidas acima também estão disponíveis aqui. Uma função adicional permite a criação de várias cópias do CD ou DVD.

Figura 9.3 *Copiando um CD*



Marque *On the fly* para gravar o CD assim que ele for lido ou selecione *Somente Criar Imagem* para criar uma imagem no caminho especificado em *Diretório Temporário → Gravar arquivo de imagem para* e grave a imagem posteriormente.

9.4 Gravando imagens ISO

Se você já tiver uma imagem ISO, vá para *Ferramentas → CD → Queimar imagem de CD*. É aberta uma janela para que você digite o local da *Imagem para Queimar*. O K3b calcula uma soma de verificação e a exibe em *Soma MD5*. Se o arquivo ISO foi obtido por download da Internet, essa soma mostrará se o download foi bem-sucedido.

Use as guias *Opções* e *Avançado* para definir suas preferências. Para gravar o CD, clique em *Iniciar*.

9.5 Criando um CD ou DVD multissessão

Os discos multissessão podem ser usados para a gravação de dados em mais de uma sessão. Isso é útil, por exemplo, no caso de gravações de backups que são menores do que a mídia. Em cada sessão, você pode adicionar outro arquivo de backup. O interessante nisso é que você não fica limitado somente a CDs ou DVDs de dados. Pode também adicionar sessões de áudio em um disco multissessão.

Para iniciar um novo disco multissessão, faça o seguinte:

1. Crie primeiro o seu disco de dados e adicione todos os arquivos. Você não pode iniciar com uma sessão de CD de áudio. Verifique se você não preencheu todo o disco, pois se tiver preenchido, não poderá acrescentar uma nova sessão.

2. Grave os seus dados usando *Projeto → Queimar*. Uma caixa de diálogo é exibida.

3. Vá para a guia *Configurações* e selecione *Iniciar Multissessão*.

4. Configure outras opções se for necessário. Consulte também a Seção 9.1, “Criando um CD de dados” (p 145).

5. Inicie a sessão de gravação com *Queimar*.

Um disco multissessão será criado após um processo de gravação bem-sucedido. Desde que haja espaço suficiente na mídia, você poderá acrescentar mais sessões se desejar.

Finalize os discos apenas se você tiver certeza de que não precisa de novas sessões ou se o espaço estiver ocupado.

NOTA: Sobre o espaço de armazenamento em disco multissessão

Esteja ciente de que discos multissessão precisam de espaço para manter todas as entradas das suas sessões. Isso resulta em uma quantidade menor de espaço disponível no disco. A quantidade depende do número de sessões.

9.6 Mais informações

Além das duas funções principais descritas acima, o K3b oferece outras funções como a criação de cópias de DVD, a leitura de dados de áudio no formato WAV, a regravação de CDs e a reprodução de música com o leitor de áudio integrado. Veja uma descrição detalhada de todos os recursos disponíveis do programa em http://k3b.sourceforge.net.

Parte IV Office

Suíte para escritórios OpenOffice.org

10

O OpenOffice.org é uma suíte avançada que oferece ferramentas para todos os tipos de tarefas de escritório, como elaboração de textos, trabalho com planilhas ou criação de gráficos e apresentações. Com o OpenOffice.org, use os mesmos dados em todas as diferentes plataformas de computação. Também é possível abrir e editar arquivos em formatos Microsoft Office e gravá-los novamente nesse formato, se necessário. Este capítulo descreve apenas as habilidades básicas que são necessárias para você começar a trabalhar com o OpenOffice.org. Inicie o aplicativo no menu do SUSE ou com o comando `ooffice`.

O OpenOffice.org compreende vários módulos de aplicativos (subprogramas) que foram desenvolvidos para interagir entre si. Esses módulos estão listados na Tabela 10.1, "Módulos de aplicativos do OpenOffice.org" (p 155). Neste capítulo, a abordagem principal é o Writer. Existe uma descrição completa de cada módulo na ajuda online, explicada na Seção 10.6, "Mais informações" (p 162).

Tabela 10.1 *Módulos de aplicativos do OpenOffice.org*

Writer	Avançado processador de textos eletrônico
Calc	Planilha eletrônica que inclui um utilitário de gráficos
Draw	Aplicativo de desenho para criação de gráficos vetoriais
Math	Aplicativo para elaboração de fórmulas matemáticas
Impress	Aplicativo para criação de apresentações

O aspecto do aplicativo varia de acordo com o gerenciador de área de trabalho ou janela usada. Além disso, são usados os formatos de caixa de diálogo para abrir e gravar na sua área de trabalho. Independentemente do aspecto, as funções e o layout básicos são os mesmos.

10.1 Compatibilidade com outros aplicativos do Office

O OpenOffice.org é capaz de funcionar com documentos, planilhas, apresentações e bancos de dados do Microsoft Office. Eles podem ser abertos sem problemas, como outros arquivos, e gravados naquele formato. Como os formatos da Microsoft são fechados e as especificidades não ficam disponíveis para outros aplicativos, eventualmente há problemas de formatação. Se você tiver problemas com os documentos, considere a possibilidade de abri-los no aplicativo original e regravá-los em um formato aberto, como RTF no caso de documentos de texto ou CSV, no caso de planilhas.

Para converter uma série de documentos, como por exemplo quando ocorre a migração para o aplicativo, selecione *Arquivo → Assistente → Conversor de Documentos*. Escolha o formato do arquivo que será convertido. Há vários formatos do StarOffice e do Microsoft Office disponíveis. Após a seleção do formato, clique em *Próximo* e especifique onde o OpenOffice.org deve procurar os modelos e documentos para conversão e o diretório em que os arquivos convertidos devem ser colocados. Antes de continuar, verifique se todas as outras configurações estão corretas. Clique em *Próximo* para ver um resumo das ações a serem executadas, oferecendo outra oportunidade para verificar se todas as configurações estão corretas. Por fim, inicie a conversão clicando em *Converter*.

IMPORTANTE: Localizando arquivos do Windows

Os documentos da partição do Windows geralmente ficam em um subdiretório de `/windows`.

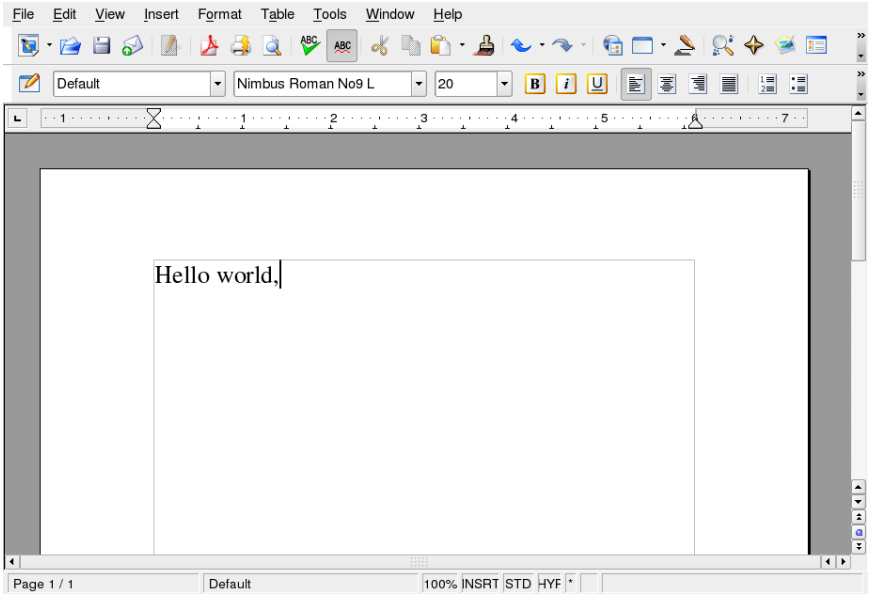
Ao compartilhar documentos, você tem várias opções. Se o destinatário somente precisar ler o documento, exporte-o para um arquivo PDF clicando em *Arquivo → Exportar*

como PDF. Os PDFs podem ser lidos em qualquer plataforma com um visualizador como o Adobe Acrobat Reader. Para compartilhar um documento para edição, use um dos formatos de documento normais. Os formatos padrão obedecem ao formato XML do padrão OASIS, tornando-os compatíveis com uma série de aplicativos. Os formatos TXT e RTF, embora limitados em termos de formatação, podem ser uma boa opção para documentos de texto. O formato CSV é útil para planilhas. O OpenOffice.org também pode oferecer o formato da preferência do seu destinatário, principalmente formatos da Microsoft.

O OpenOffice.org está disponível para uma série de sistemas operacionais. Isso faz dele uma excelente ferramenta quando um grupo de usuários precisa compartilhar arquivos com freqüência e não utiliza o mesmo sistema operacional.

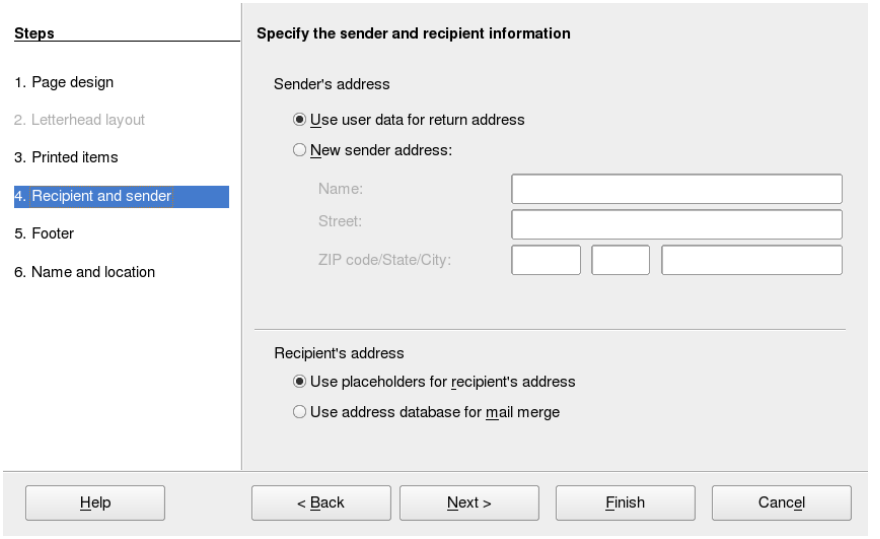
10.2 Processamento de texto com o Writer

Figura 10.1 *OpenOffice.org Writer*



Há duas maneiras de criar um documento. Para criar um documento totalmente novo, use *Arquivo → Novo → Documento de Texto*. Para utilizar um formato padrão e elementos predefinidos em seus documentos, use um assistente. Os assistentes são pequenos utilitários que permitem tomar algumas decisões básicas e criar um documento "pronto para o uso" a partir de um modelo. Por exemplo, para criar uma carta comercial, selecione *Arquivo → Assistentes → Carta*. Usando as caixas de diálogo do assistente, crie um documento básico com facilidade usando um formato padrão. Uma caixa de diálogo de um assistente é mostrada na Figura 10.2, "Assistente do OpenOffice.org" (p 158).

Figura 10.2 *Assistente do OpenOffice.org*



Digite texto na janela do documento de acordo com sua preferência. Use a barra de ferramentas *Formatação* ou o menu *Formato* para ajustar a aparência do documento. Use o menu *Arquivo* ou os botões pertinentes da barra de ferramentas para imprimir e gravar o documento. Com as opções de *Inserir*, adicione itens extras ao documento, como uma tabela, uma imagem ou um gráfico.

10.2.1 Selecionando texto

Para selecionar texto, clique no início da seleção desejada e, com o botão do mouse pressionado, mova o cursor até o fim da seleção (que pode ser caracteres, linhas ou

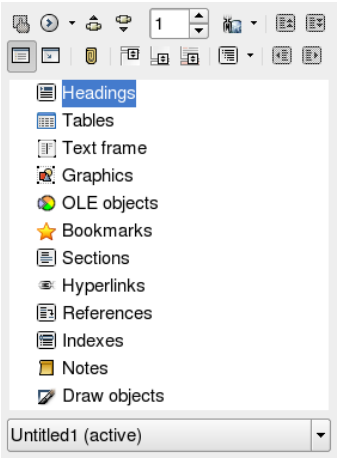
parágrafos inteiros). Solte o botão quando todo o texto desejado estiver selecionado. Enquanto estiver selecionado, o texto será exibido com as cores invertidas. Clique o botão direito do mouse na seleção para abrir um menu de contexto. Use o menu de contexto para mudar a fonte e seu estilo, além de outras propriedades do texto.

O texto selecionado pode ser cortado ou copiado para a área de transferência. O texto cortado ou copiado pode ser colado de volta em outro local do documento. Use o menu de contexto, *Editar*, ou os ícones da barra de ferramentas pertinentes para acessar essas funções.

10.2.2 Navegando em documentos grandes

O Navigator exibe informações sobre o conteúdo dos documentos. Ele também permite que você acesse rapidamente os diversos elementos incluídos. Por exemplo, use o Navigator para ter uma visão geral de todos os capítulos ou para ver uma lista das imagens incluídas no documento. Para abri-lo, selecione *Editar* → *Navigator*. A Figura 10.3, "Navigator no Writer" (p 159) mostra o Navigator em ação. Os elementos relacionados no Navigator variam de acordo com o documento carregado no Writer.

Figura 10.3 *Navigator no Writer*



10.2.3 Formatando com estilos

A caixa de diálogo que se abre com *Formato → Estilos e Formatação* pode ajudá-lo a formatar o texto de inúmeras maneiras. Se você definir *Automático* na lista suspensa na parte inferior dessa caixa de diálogo, o OpenOffice.org oferecerá uma seleção de estilos adaptados à tarefa em questão. Se você selecionar *Todos os Estilos*, o Stylist oferecerá todos os estilos do grupo ativo. Selecione os grupos com os botões da parte superior.

Ao usar esse método para formatar seu texto, chamado *formatação automática*, o texto não é formatado diretamente. Em vez disso, um estilo é aplicado. O estilo pode ser modificado com facilidade, automaticamente resultando em uma mudança de formatação de todo o texto ao qual ele está designado.

Para designar um estilo a um parágrafo, selecione o estilo a ser usado e clique no ícone em forma de lata de tinta em *Estilos e Formatações*. Clique nos parágrafos aos quais o estilo será designado. Para interromper a designação do estilo, pressione a tecla Esc ou clique no ícone de tinta novamente.

Crie com facilidade seus próprios estilos formatando um parágrafo ou caractere como desejar, usando o menu *Formatar* ou a barra de ferramentas. Selecione o item formatado do qual o estilo deve ser copiado. Em seguida, clique e mantenha o botão à direita da lata de tinta pressionado em *Estilos e Formatação* em selecionar *Novo Estilo da Seleção* no menu que é aberto. Digite um nome para o estilo e clique em *OK*. Esse estilo pode então ser aplicado a outros textos.

Para mudar detalhes de um estilo, selecione o estilo na lista, clique o botão direito do mouse nele e selecione *Modificar* no menu. Será aberta uma caixa de diálogo com todas as possíveis propriedades de formatação disponíveis para modificação.

10.3 Apresentando o Calc

O Calc é o aplicativo de planilhas do OpenOffice. Crie uma nova planilha com *Arquivo → Novo → Planilha*ou abra uma com *Arquivo → Abrir*. A leitura e gravação do Calc podem ser feitas no formato Microsoft Excel.

Nas células da planilha, digite dados fixos ou fórmulas. Uma fórmula pode manipular dados de outras células para gerar um valor para a célula em que está inserida. Também é possível criar gráficos a partir de valores de células.

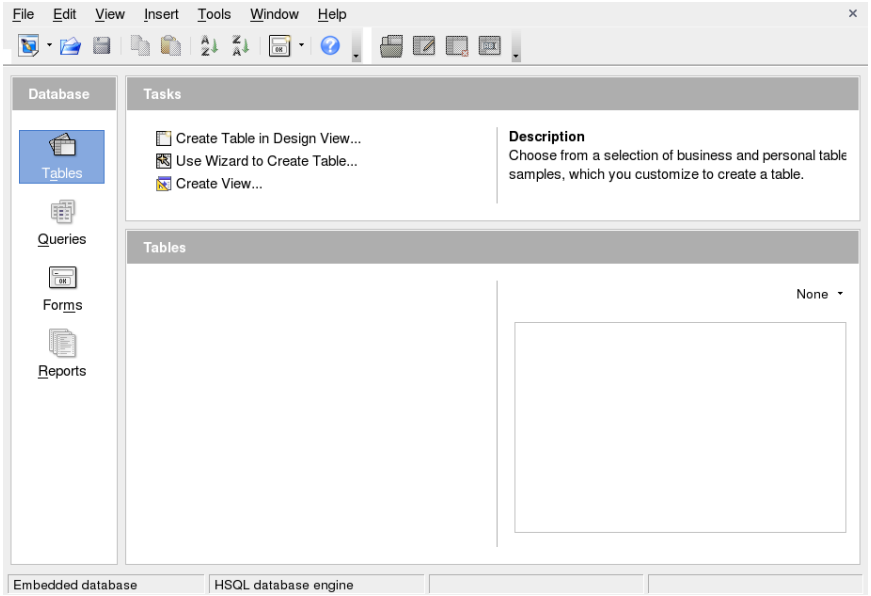
10.4 Apresentando o Impress

O Impress foi projetado para a criação de apresentações para exibição na tela ou impressão, como transparências. Crie uma apresentação da estaca zero com *Arquivo → Novo → Apresentação*. Para criar uma apresentação com a ajuda de um assistente, use *Arquivo → Assistentes → Apresentação*. Abra uma apresentação existente com *Arquivo → Abrir*. O Impress pode abrir e gravar apresentações do Microsoft PowerPoint.

10.5 Apresentando o Base

O OpenOffice 2.0 apresenta um novo módulo de banco de dados. Crie um banco de dados com *Arquivo → Novo → Banco de Dados*. Um assistente se abrirá para ajudar na criação do banco de dados. O Base também pode funcionar com os bancos de dados do Microsoft Access.

Figura 10.4 *Base — bancos de dados do OpenOffice.org*



Tabelas, formulários, consultas e relatórios podem ser criados manualmente ou por meio de um prático assistente. Por exemplo, o assistente de tabela contém uma série de campos comuns para negócios e uso pessoal. Os bancos de dados criados no Base podem ser usados como fontes de dados, como por exemplo durante a criação de cartas.

10.6 Mais informações

O OpenOffice.org inclui uma série de opções de informação, que prestam quatro diferentes níveis de informação. Para saber tudo sobre um tópico, selecione *Ajuda → Ajuda do OpenOffice.org*. O sistema de ajuda fornece informações detalhadas sobre cada módulo do OpenOffice.org (Writer, Calc, Impress e outros).

Quando o aplicativo é iniciado pela primeira vez, ele dá *Dicas*, informações breves sobre botões quando o mouse passa sobre eles, e o *Agente de Ajuda*, informações baseadas em ações realizadas. Para obter informações sobre botões mais completas do que as informações das *Dicas*, use a *Ajuda → O que é isso?* e, em seguida, passe o mouse sobre os botões desejados. Para terminar o modo *O que é Isso*, clique. Se você precisar dessa função com freqüência, considere a ativação de *Dicas* em *Ferramentas*

→ *Opções* → *OpenOffice.org* → *Geral*. O *Agente de Ajuda* e as *Dicas* também podem ser ativados e desativados aqui.

O Website do OpenOffice.org é o seguinte: `http://www.openoffice.org`. Lá, procure listas de discussão, artigos e informações sobre defeitos. O site oferece versões de diversos sistemas operacionais para download.

11 Evolution: programa de e-mail e calendário

O Evolution é uma suíte de groupware que oferece os recursos comuns de e-mail com recursos estendidos, como listas de tarefas e um calendário. O aplicativo também fornece um bloco de endereços completo que inclui a capacidade de enviar informações de contato para outras pessoas no formato vCard.

Inicie o Evolution do menu principal ou com `evolution`. Quando iniciado pela primeira vez, o Evolution oferece um assistente de configuração. Seu uso é descrito na Seção 11.3.1, “Configurando contas” (p 167).

IMPORTANTE: Contas do Microsoft Exchange

Para usar o Evolution com o Microsoft Exchange, você deve instalar o pacote `ximian-connector`. Instale-o com o YaST.

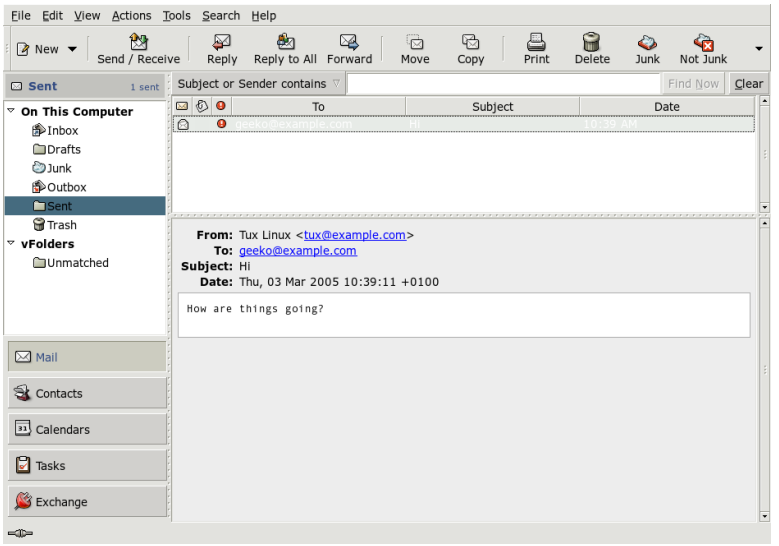
11.1 Importando e-mails de outros programas de e-mail

Para importar mensagens de outros programas de e-mail, como o Netscape, selecione *File* → *Import* (Arquivo - Importar). Para formatos mbox, selecione *Import a single file* (Importar um único arquivo). No Netscape, selecione *Import data and settings from older programs* (Importar dados e configurações de programas mais antigos). Para trabalhar com dados de programas usando o formato maildir, como KMail, configure uma conta para acessar o diretório de e-mails.

11.2 Visão geral sobre o Evolution

A janela padrão é mostrada na Figura 11.1, “Janela do Evolution com e-mail” (p 166). Os menus, itens de menu e ícones disponíveis na barra de ferramentas variam de acordo com o componente aberto. Use o quadro esquerdo para selecionar as informações a serem exibidas no quadro direito. Ajuste o tamanho dos quadros arrastando as barras divisoras.

Figura 11.1 *Janela do Evolution com e-mail*



11.2.1 Correio

Nesta tela, a parte superior da janela mostra o conteúdo da pasta atual. A parte inferior é um painel de visualização destinado a exibir a mensagem de e-mail selecionada. Para exibir outra pasta, selecione-a na lista de pastas no quadro esquerdo.

Use a barra de pesquisa para pesquisar as mensagens em uma pasta. Para classificar as mensagens pelo cabeçalho de uma tabela, clique no cabeçalho desejado. A seta à direita mostra se a coluna é classificada na ordem crescente ou decrescente. Clique no cabeçalho da coluna até as mensagens sejam classificadas na direção desejada.

11.2.2 Contatos

Esta tela mostra todos os endereços do bloco de endereços. Para localizar um endereço específico, use a barra de pesquisa ou clique no botão à direita para exibir a primeira letra do sobrenome do contato. Adicione contatos ou listas com a barra de ferramentas.

11.2.3 Calendário

A exibição inicial mostra uma tela do dia atual com o mês e uma lista de tarefas mostrada em um painel adicional à direita. As telas de semana, semana de trabalho e mês também estão disponíveis na barra de ferramentas ou no menu *View* (Exibir). Use a barra de pesquisa para encontrar um compromisso digitado no calendário. Adicione compromissos e tarefas usando os botões da barra de ferramentas. Você também pode usar a barra de ferramentas para percorrer o calendário ou ir para uma data específica.

11.2.4 Tarefas

A opção *Tasks* (Tarefas) fornece uma lista de tarefas. Os detalhes da tarefa selecionada são mostrados na parte inferior da janela. Use *File* → *New* → *Task* (Arquivo - Novo - Tarefa) para adicionar uma nova tarefa. Pesquise as tarefas com a barra de pesquisa. Para designar tarefas a outras pessoas, clique o botão direito nas tarefas e selecione *Assign Task* (Designar Tarefa). Use a opção *Open* (Abrir) para abrir a tarefa e adicionar mais detalhes, como uma data de vencimento e o status de conclusão.

11.3 Correio

O componente de correio do Evolution pode funcionar com várias contas em diversos formatos. Ele oferece recursos úteis, como pastas virtuais para a exibição de resultados de pesquisa e a filtragem de mensagens indesejadas. Configure o aplicativo em *Edit* → *Preferences* (Editar - Preferências).

11.3.1 Configurando contas

O Evolution pode recuperar e-mails de várias contas de e-mail. A conta a partir da qual você deseja enviar e-mails pode ser selecionada quando você redige uma mensagem.

Configure as contas de e-mail em *Edit → Preferences → Mail Accounts* (Editar - Preferências - Contas de Correio). Para modificar uma configuração existente, selecione-a e clique em *Edit* (Editar). Para apagar uma conta, selecione-a e clique em *Delete* (Apagar).

Para adicionar uma nova conta, clique em *Add* (Adicionar). Esse procedimento abre o assistente de configuração. Clique em *Forward* (Encaminhar) para usá-lo. Digite seu nome e endereço de e-mail nos respectivos campos. Se desejar, digite as informações opcionais. Marque *Make this my default account* (Tornar esta a minha conta padrão) para usar essa conta por padrão ao criar e-mails. Clique em *Forward* (Encaminhar).

Selecione o formato de e-mail recebido adequado para esse endereço em *Server Type* (Tipo de Servidor). *POP* é o formato mais comum para fazer download de e-mails em um servidor remoto. *IMAP* funciona com pastas de correio em um servidor especial. Obtenha essas informações com o provedor de serviços de Internet ou com o administrador do sistema. Preencha os outros campos relevantes exibidos quando o tipo de servidor é selecionado. Quando terminar, clique em *Forward* (Encaminhar). Selecione as *Receiving Options* (Opções de Recebimento) desejadas, se disponíveis. Clique em *Forward*.

Depois, configure as opções de entrega de e-mail. Para submeter os e-mails enviados ao sistema local, selecione *Sendmail*. Para um servidor remoto, selecione *SMTP*. Obtenha essas informações com o provedor de serviços de Internet ou com o administrador do sistema. Para SMTP, preencha os outros campos exibidos após a seleção. Quando terminar, clique em *Forward*.

Por padrão, o endereço de e-mail é usado como o nome de identificação da conta. Digite outro nome se desejar. Clique em *Forward*. Clique em *Apply* (Aplicar) para gravar a configuração da conta.

Para tornar uma conta o padrão para o envio de e-mails, selecione a conta desejada e pressione *Default* (Padrão). Para desabilitar a recuperação de e-mails de uma conta, selecione-a e clique em *Disable* (Desabilitar). Uma conta desabilitada ainda pode ser usada como o endereço de envio, mas ela não é verificada em relação aos e-mails recebidos. Se necessário, reative a conta com *Enable* (Habilitar).

11.3.2 Criando mensagens

Para criar uma nova mensagem, clique em *New → Mail Message* (Nova - Mensagem de E-mail). Se uma mensagem for respondida ou encaminhada, o mesmo editor de mensagens será aberto. Ao lado de *From* (De), selecione a conta da qual a mensagem será enviada. Nos campos de destinatário, digite um endereço de e-mail ou parte de um nome ou endereço contido no seu bloco de endereços. Se for encontrada uma correspondência no bloco de endereços para o que foi digitado, uma lista de opções será exibida. Clique no contato desejado ou conclua sua entrada se não houver correspondências. Para selecionar um destinatário diretamente no bloco de endereços, clique em *To* (Para) ou *CC*.

O Evolution pode enviar e-mails como texto simples ou HTML. Para formatar e-mails em HTML, selecione *Format* (Formatar) na barra de ferramentas. Para enviar anexos, selecione *Attach* (Anexar) ou *Insert → Attachment* (Inserir - Anexo).

Para enviar a mensagem, clique em *Send* (Enviar). Se ainda não estiver pronto para enviá-la imediatamente, faça outra seleção em *File* (Arquivo). Por exemplo, grave a mensagem como rascunho ou envie-a posteriormente.

11.3.3 E-Mail criptografado e assinaturas

O Evolution suporta a criptografia de e-mails com PGP. Ele pode assinar e-mails e verificar as mensagens de e-mail assinadas. Para usar esses recursos, gere e gerencie chaves com um aplicativo externo, como gpg ou KGpg.

Para assinar a mensagem de e-mail antes de enviá-la, selecione *Security → PGP Sign* (Segurança - Assinatura PGP). Quando você clica em *Send* (Enviar), uma caixa de diálogo solicita a senha de sua chave secreta. Digite a senha e saia da caixa de diálogo com *OK* para enviar o e-mail assinado. Para assinar outras mensagens de e-mail durante esta sessão sem precisar "desbloquear" a chave secreta repetidamente, marque *Remember this password for the remainder of this session* (Lembrar esta senha no restante desta sessão).

Quando você recebe e-mails assinados de outros usuários, um pequeno ícone de cadeado aparece no final da mensagem. Se você clicar nesse símbolo, o Evolution iniciará um programa externo (gpg) para verificar a assinatura. Se a assinatura for válida, uma marca de seleção verde aparecerá ao lado do símbolo. Se a assinatura for inválida, aparecerá um cadeado quebrado.

Também é muito fácil criptografar e descriptografar e-mails. Após redigir uma mensagem de e-mail, vá para *Security → PGP encrypt* (Segurança - Criptografia PGP) e envie-a. Quando você recebe mensagens criptografadas, uma caixa de diálogo solicita a senha de sua chave secreta. Digite a frase secreta para descriptografar a mensagem de e-mail.

11.3.4 Pastas

Em geral, é conveniente classificar as mensagens de e-mail em várias pastas. A árvore de pastas é mostrada no quadro esquerdo. Se os e-mails forem acessados através do IMAP, as respectivas pastas também serão mostradas nessa barra de pastas. Para POP e a maioria dos outros formatos, as pastas são armazenadas localmente e classificadas em *Local Folders* (Pastas Locais).

Várias pastas estão incluídas por padrão. *Inbox* (Caixa de Entrada) é o local onde novas mensagens obtidas de um servidor são inicialmente colocadas. *Sent* (Enviados) é usado para gravar cópias de mensagens de e-mail enviadas. A *Outbox* (Caixa de Saída) fornece armazenamento temporário para e-mails que ainda não foram enviados. Ela será útil se você estiver trabalhando offline ou se o servidor de correio de saída estiver temporariamente inacessível. *Drafts* (Rascunhos) é usado para gravar cópias de mensagens de e-mail inacabadas. A pasta *Trash* (Lixo) destina-se ao armazenamento temporário de itens apagados. *Junk* (Mensagens Indesejadas) destina-se ao recurso de filtragem de mensagens indesejadas do Evolution.

É possível criar novas pastas em *On This Computer* (Neste Computador) ou como subpastas de pastas existentes. Crie uma hierarquia de pastas com a complexidade desejada. Para criar uma nova pasta, selecione *File → New → Mail Folder* (Arquivo - Novo - Pasta de E-mails). Na caixa de diálogo Mail Folder, digite um nome para a nova pasta. Use o mouse para determinar a pasta-pai na qual colocar a nova pasta. Clique em *OK* para sair da caixa de diálogo.

Para mover uma mensagem para uma pasta, selecione a mensagem. Clique o botão direito do mouse para abrir o menu de contexto. Selecione *Move to Folder* (Mover para Pasta) e, na caixa de diálogo exibida, a pasta de destino. Clique em *OK* para mover a mensagem. O cabeçalho da mensagem na pasta original é mostrado com uma linha atravessada, significando que a mensagem está marcada para ser apagada dessa pasta. A mensagem é armazenada na nova pasta. É possível copiar mensagens de uma maneira semelhante.

A transferência manual de diversas mensagens para pastas diferentes pode ser demorada. É possível usar filtros para automatizar esse procedimento.

11.3.5 Filtros

O Evolution oferece diversas opções para a filtragem de e-mails. É possível usar filtros a fim de mover uma mensagem para uma pasta específica ou para apagar uma mensagem. Também é possível mover mensagens diretamente para a lixeira com um filtro. Há duas opções para criar um novo filtro: criá-lo do zero ou com base em uma mensagem a ser filtrada. A última opção é muito útil para a filtragem de mensagens enviadas para uma lista de discussão.

Configurando um filtro

Selecione *Ferramentas → Filtros*. Essa caixa de diálogo lista os filtros existentes, que podem ser editados ou apagados. Clique em *Add* (Adicionar) para criar um novo filtro. Como alternativa, para criar um filtro com base em uma mensagem, selecione-a e, em seguida, selecione *Tools → Create Filter from Message* (Ferramentas - Criar Filtro a Partir de Mensagem).

Digite um nome para o novo filtro em *Rule Name* (Nome da Regra). Selecione os critérios a serem usados para o filtro. A opções são: remetente, destinatários, conta de origem, assunto, data e status. A caixa suspensa mostrando *Contains* (Contém) oferece várias opções, como *contains* (contém), *is* (é) e *is not* (não é). Selecione a condição adequada. Digite o texto pelo qual pesquisar. Clique em *Add* (Adicionar) para adicionar mais critérios de filtragem. Use *Execute actions* (Executar ações) para determinar se todos os critérios ou somente alguns devem ser atendidos para que o filtro seja aplicado.

Na parte inferior da janela, determine a ação a ser executada quando os critérios de filtragem forem atendidos. É possível, por exemplo, mover ou copiar as mensagens para uma pasta ou atribuir-lhes uma cor especial. Ao movê-las ou copiá-las, clique para selecionar a pasta de destino. Na lista de pastas exibida, selecione a pasta. Para criar uma nova pasta, clique em *New* (Nova). Clique em *OK* quando a pasta correta for selecionada. Ao terminar de criar o filtro, clique em *OK*.

Aplicando filtros

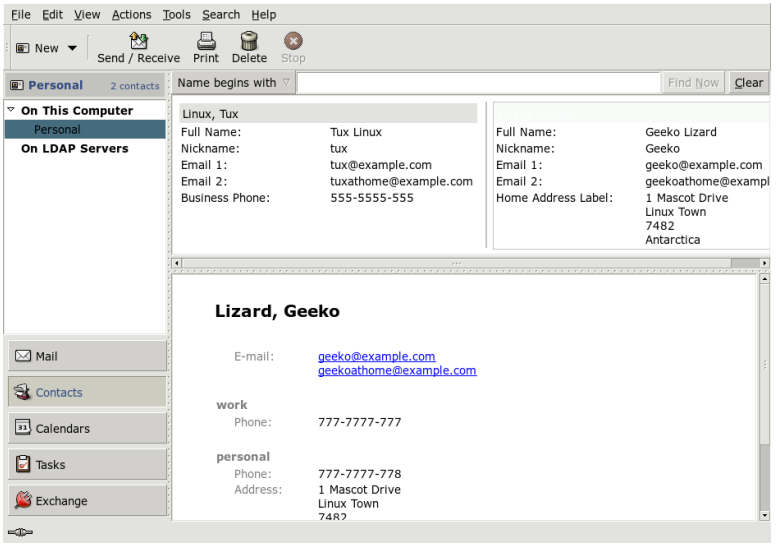
Os filtros são aplicados na ordem listada na caixa de diálogo acessada com *Tools* → *Filters* (Ferramentas - Filtros). Para mudar a ordem, realce um filtro e clique em *Up* (Para Cima) ou *Down* (Para Baixo). Ao terminar, clique em *OK* para fechar a caixa de diálogo de filtro.

Os filtros são aplicados a todas as novas mensagens de e-mail. Eles não são aplicados aos e-mails já contidos nas pastas. Para aplicar filtros às mensagens já recebidas, selecione as mensagens desejadas e, em seguida, *Actions* → *Apply Filters* (Ações - Aplicar Filtros).

11.4 Contatos

O Evolution pode usar vários blocos de endereços. Os blocos disponíveis são listados no quadro esquerdo. Pesquise um contato específico usando a barra de pesquisa. Adicione contatos em vários formatos ao bloco de endereços do Evolution usando *File* → *Import* (Arquivo - Importar). Clique o botão direito do mouse em um contato para abrir um menu de opções a serem selecionadas, como encaminhar o contato ou gravá-lo como vCard. Clique duas vezes em um contato para editá-lo.

Figura 11.2 *Bloco de endereços do Evolution*



11.4.1 Adicionando contatos

Juntamente com o nome e o endereço de e-mail, o Evolution pode armazenar outras informações de endereço e de contato sobre uma pessoa. Adicione rapidamente o endereço de e-mail de um remetente clicando o botão direito no endereço marcado na visualização da mensagem. Para digitar um contato totalmente novo, clique em *New Contact* (Novo Contato) na tela *Contacts* (Contatos). Os dois métodos abrem uma caixa de diálogo na qual as informações de contato podem ser digitadas.

Na guia *Contact* (Contato), digite o nome do contato, os endereços de e-mail, os números de telefone e as identidades de mensagens instantâneas. A opção *Personal Information* (Informações Pessoais) destina-se a endereços da Web e outras informações detalhadas. Digite as outras informações de endereço do contato em *Mailing Address* (Endereço para Correspondência). Após digitar todos os detalhes desejados para o contato, clique em *OK* para adicioná-lo ao bloco de endereços.

11.4.2 Criando uma lista

Se você envia mensagens de e-mail com freqüência para um grupo de pessoas, pode simplificar o processo criando uma lista com esses endereços. Clique em *File → New → Contact List* (Arquivo - Novo - Lista de Contatos). O editor de lista de contatos é aberto. Digite um nome para a lista. Para adicionar um endereço, digite-o na caixa e clique em *Add* (Adicionar) ou arraste os contatos da tela *Contacts* (Contatos) e solte-os na caixa. Alterne para *Hide addresses* (Ocultar endereços) para selecionar se os destinatários devem ver as outras pessoas que receberam o e-mail. Quando terminar, clique em *OK*. Agora, a lista é um dos seus contatos e aparece na janela de composição após a digitação das primeiras letras.

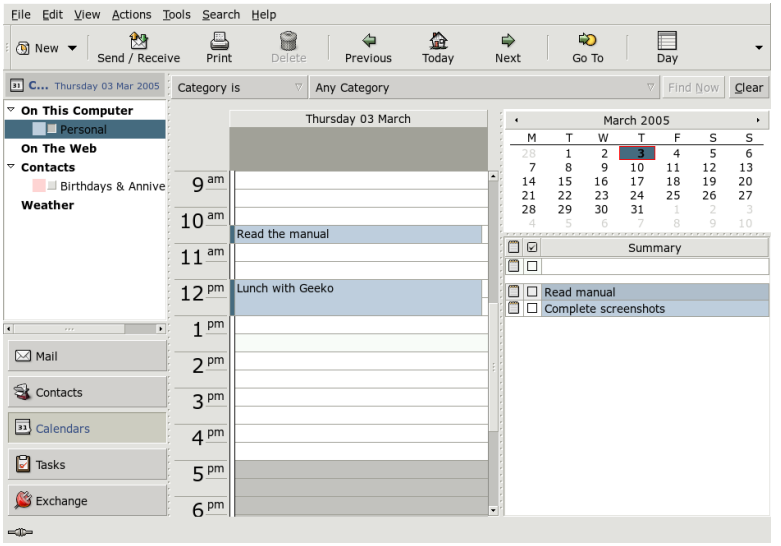
11.4.3 Adicionando blocos de endereços

Configurar blocos de endereços adicionais do GroupWise e Exchange na configuração dessa conta. Para adicionar outros blocos LDAP ou locais, selecione *File → New → Address Book* (Arquivo - Novo - Bloco de Endereços). Na caixa de diálogo exibida, selecione o tipo de bloco de endereços e digite as informações necessárias.

11.5 Calendários

O Evolution pode trabalhar com vários calendários. Com *File → Import* (Arquivo - Importar), importe calendários no formato iCalendar. Use o calendário para digitar compromissos e programar reuniões com outras pessoas. Se desejar, defina lembretes para que você saiba quando começarão os compromissos programados.

Figura 11.3 *Calendário do Evolution*



11.5.1 Adicionando compromissos

Para adicionar um novo compromisso ao calendário, clique em *File* → *New* → *Appointment* (Arquivo - Novo - Compromisso). Na guia *Appointment* (Compromisso), digite os detalhes do compromisso. Se desejar, selecione uma categoria para facilitar a pesquisa e classificação posteriores. Opcionalmente, use *Alarm* para definir um alarme para que você seja lembrado antes do início do compromisso. Se o compromisso ocorrer com regularidade, defina as datas recorrentes em *Recurrence* (Recorrência). Clique em *OK* depois de fazer todas as configurações. Em seguida, o novo compromisso é mostrado no calendário.

11.5.2 Programando uma reunião

Para programar uma reunião com outras pessoas, selecione *File* → *New* → *Meeting* (Arquivo - Novo - Reunião). Digite informações como faria para um compromisso. Adicione os participantes em *Invitations* (Convites) ou *Scheduling* (Programação). Para digitar os participantes do seu bloco de endereços, use *Contacts* (Contatos) para abrir uma lista dos contatos no bloco. A opção *Scheduling* (Programação) também pode ser usada para programar um horário que se ajuste a todos os participantes. Para encontrar

um horário de forma automática, pressione *Autopick* (Escolher Automaticamente) depois de configurar os participantes.

11.5.3 Adicionando calendários

Os calendários do GroupWise e Exchange devem ser definidos na configuração da conta. Para adicionar outros calendários locais ou da Web, selecione *File → New → Calendar* (Arquivo - Novo - Calendário). Selecione o tipo desejado e digite as informações necessárias.

11.6 Sincronizando dados com dispositivos portáteis

O Evolution foi projetado para que seus dados possam ser sincronizados com dispositivos portáteis, como um Palm. A sincronização usa o GNOME Pilot. Selecione *Tools → Pilot Settings* (Ferramentas - Configurações do Piloto) para abrir o assistente de configuração. Consulte a Ajuda para obter mais informações.

11.7 Evolution para usuários do GroupWise

Os usuários do GroupWise não devem ter muitos problemas em usar o Evolution para acessar suas contas do GroupWise. O Evolution e o GroupWise usam uma terminologia bem semelhante. Os usuários familiarizados com um sistema devem conseguir aprender a usar o outro com esforço mínimo.

11.7.1 Configurando o Evolution para acessar o sistema GroupWise

Use o assistente de configuração de e-mail do Evolution para configurar o acesso deste ao sistema GroupWise. Para iniciar o assistente, clique em *Preferences → Mail Accounts → Add* (Preferências - Contas de E-mail - Adicionar) e clique em *Forward* (Encaminhar).

Na página Identity (Identidade), forneça seu endereço de e-mail no sistema GroupWise (por exemplo, joe@example.com) e clique em *Forward* (Encaminhar).

Na página Receiving Email (Recebendo E-mails), selecione *IMAP* na lista Server Type (Tipo de Servidor), especifique o nome do host do servidor GroupWise no campo Host, defina as outras configurações na página Receiving Options (Opções de Recebimento) da maneira adequada para o sistema e clique em *Forward* (Encaminhar).

Na página Receiving Email (Recebendo E-mails), selecione *SMTP* na lista Server Type (Tipo de Servidor), especifique o nome do host do servidor GroupWise no campo Host, defina as outras opções em Sending Email (Enviando E-mails) da maneira adequada para o sistema e clique em *Forward* (Encaminhar).

Na página Account Management (Gerenciamento de Contas), especifique o nome que deseja usar para identificar a conta na página Evolution Settings (Configurações do Evolution) e clique em *Forward* (Encaminhar).

Clique em *Apply* (Aplicar) para criar a conta do GroupWise. Agora, a caixa de correio do GroupWise será exibida na lista de contas de e-mail disponíveis.

11.8 Para obter mais informações

O Evolution oferece páginas de ajuda interna abrangente. Use o menu *Help* (Ajuda) para acessar essas informações. Para obter mais informações sobre o Evolution, consulte o site do projeto em `http://www.gnome.org/projects/evolution/`.

Kontact: um programa de e-mail e calendário

12

O Kontact combina a funcionalidade de vários aplicativos do KDE em uma única interface conveniente para o gerenciamento de informações pessoais. Esses aplicativos incluem KMail para e-mail, KOrganizer para calendário, KAddressbook para contatos e KNotes para notas. Também é possível sincronizar dados com dispositivos externos como um PalmPilot ou outro dispositivo portátil. O Kontact é facilmente integrado com o restante da área de trabalho do KDE e se conecta a diversos servidores de groupware. Ele inclui recursos extras, como filtragem de spam e de vírus e um leitor RSS.

Inicie o Kontact no menu principal com *Office → Kontact (Personal Information Manager)*. Outra opção é digitar `kontact` na linha de comando. Você também pode abrir os componentes individuais em vez do aplicativo combinado se precisar somente de funcionalidade parcial.

12.1 Importando e-mail de outros programas de mensagens

Para importar um e-mail de outros aplicativos, selecione *Ferramentas → Importar Mensagens* na tela de mensagens do Kontact. Ele contém filtros de importação para Outlook Express, formato mbox, formato de texto de e-mail, Pegasus Mail, Opera, Evolution, além de outros. O utilitário de importação também pode ser iniciado separadamente com o comando `kmailcvt`.

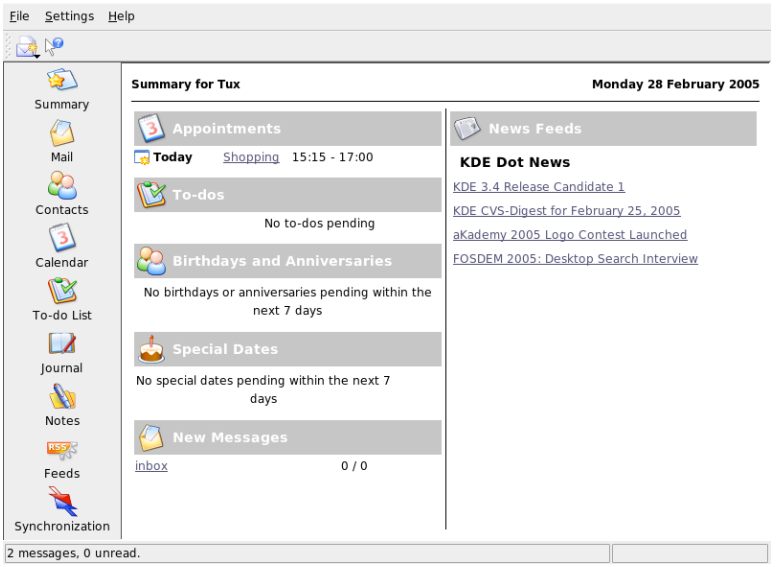
Selecione o aplicativo correspondente e confirme com *Continuar*. Um arquivo ou pasta deve ser especificado, dependendo do tipo selecionado. Em seguida, o Kontact conclui o processo.

12.2 Visão geral do Kontact

A tela da janela padrão, que mostra o *Resumo*, é exibida na Figura 12.1, “Janela do Kontact que mostra o Resumo” (p 180). Use os botões na seção à esquerda para acessar os diferentes componentes.

O *Resumo* fornece informações básicas, que incluem tarefas e aniversários futuros, informações sobre meteorologia e o status do KPilot. A seção de notícias pode acessar fontes jornalísticas RSS para fornecer notícias atualizadas que sejam do seu interesse. Use *Configurações → Configurar Tela de Resumo* para configurar a informação exibida.

Figura 12.1 *Janela do Kontact que mostra o Resumo*



12.2.1 Correio

A área de pastas, localizada à esquerda na tela, contém uma relação de todas as pastas de mensagens (caixas postais), indicando o número total de mensagens e quantas delas ainda não foram lidas. Clique em uma pasta para selecioná-la. As mensagens dessa pasta aparecerão no quadro superior direito. O número de mensagens dessa pasta também é exibido na barra de status localizada na parte inferior da janela do aplicativo.

Itens como assunto, remetente e hora de recebimento de cada mensagem são relacionados na área de cabeçalho, à direita na tela. Clique na mensagem para selecioná-la e exibi-la na janela de mensagem. Classifique as mensagens clicando em um dos cabeçalhos das colunas (assunto, remetente, data, etc.). O conteúdo da mensagem selecionada no momento é exibido no quadro de mensagens da janela. Os anexos são representados em forma de ícones no fim da mensagem, de acordo com o seu tipo MIME, ou podem ser exibidos em linha.

As mensagens podem ser marcadas com diferentes flags de status. Mude o status com *Mensagem → Marcar Mensagem*. Você pode usar esse recurso para atribuir um status a uma mensagem, como importante ou ignorada. Por exemplo, você pode realçar mensagens importantes das quais você precisa se lembrar. Exiba somente mensagens com um determinado status usando *Status* na barra de pesquisa.

12.2.2 Contatos

O quadro superior esquerdo deste componente mostra todos os endereços dos blocos de endereços ativados no momento. O quadro inferior esquerdo relaciona os blocos de endereços e mostra se cada um deles está ativo no momento. O quadro direito mostra o contato selecionado no momento. Use a barra de pesquisa na parte superior para encontrar um determinado contato.

12.2.3 Lista de pendências

A *Lista de Pendências* mostra a sua lista de tarefas. Clique no campo localizado na parte superior para adicionar um novo item à lista. Clique com o botão direito do mouse na coluna de um item existente para fazer mudanças no valor dessa coluna. Um item pode ser dividido em vários subitens. Clique com o botão direito do mouse e selecione

Nova Subtarefa para criar um subitem. Você também pode atribuir pendências a outras pessoas.

12.2.4 Calendário

A tela do calendário é dividida em diversos quadros. Por padrão, é exibido um pequeno calendário do mês atual e uma tela da semana atual. Também podem ser encontradas uma lista de pendências, uma tela detalhada da pendência ou do evento atual e uma lista de calendários com o status de cada um. Selecione uma outra tela na barra de ferramentas ou no menu *Ver*.

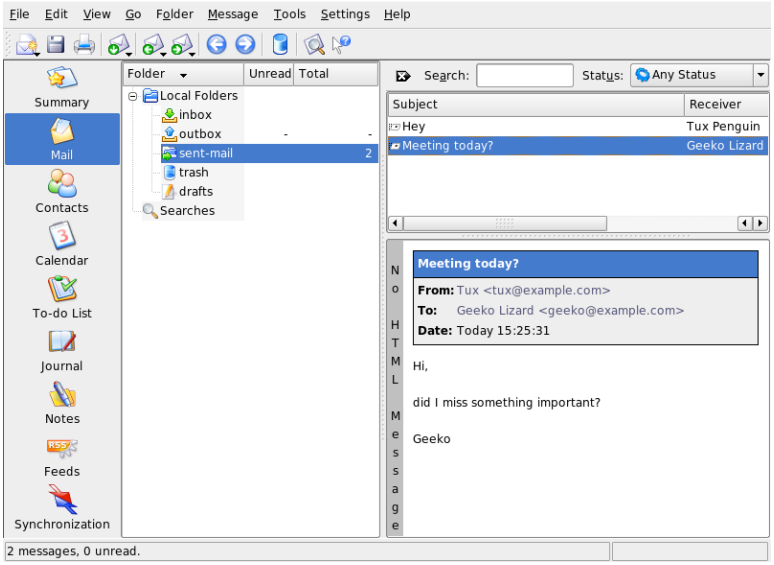
12.2.5 Notas

Use o componente Notas para manter as notas com você. Se você estiver usando o KDE, torne as suas notas visíveis na área de trabalho por meio do ícone do KNote, localizado na bandeja do sistema.

12.3 Correio

O Kontact usa o KMail como seu componente de e-mail. Para configurá-lo, abra o componente de e-mail e, em seguida, selecione *Configurações → Configurar KMail*. O KMail é um cliente de e-mail com uma variedade de recursos que suporta diversos protocolos. *Ferramentas* contém várias ferramentas úteis para gerenciar e-mails indesejados. Use *Localizar* para realizar uma pesquisa detalhada nas mensagens. O *Assistente Antispam* pode ajudá-lo a gerenciar ferramentas para filtrar e-mails comerciais indesejados. O *Assistente Antivírus* ajuda a gerenciar scanners de vírus de e-mail. Esses dois assistentes funcionam com software externo de spam e vírus. Se as opções estiverem desabilitadas, instale pacotes adicionais para a proteção contra spam e vírus.

Figura 12.2 *O componente de e-mail do Kontact*



12.3.1 Configurando contas

O Kontact pode gerenciar várias contas de e-mail, como seus endereços de e-mail particular e comercial. Ao redigir um e-mail, selecione uma das identidades definidas previamente, clicando em *Ver → Identidade*. Para criar o perfil de uma nova identidade, selecione *Configurações → Configurar KMail* e, em seguida, *Identidades → Nova*. Na caixa de diálogo que é aberta, atribua um nome à nova identidade como “particular” ou “escritório”. Clique em *OK* para abrir uma caixa de diálogo na qual você digitará informações adicionais. Você também pode atribuir uma identidade a uma pasta de forma que, ao responder a uma mensagem dessa pasta, a identidade atribuída seja selecionada.

Em *Geral*, digite seu nome, organização e endereço de e-mail. Em *Criptografia*, selecione as teclas para enviar mensagens assinadas digitalmente ou criptografadas. Para que os recursos de criptografia funcionem, crie primeiro uma chave com KGpg, como descrito no Capítulo 6, *Criptografia com KGpg* (p 103).

Em *Avançado*, você pode digitar uma resposta e um endereço de cópia oculta, escolher um dicionário, selecionar as pastas para os rascunhos e as mensagens enviadas, e definir

como as mensagens devem ser enviadas. Em *Assinatura*, decida se cada uma das suas mensagens deve ser assinada e a forma como devem ser assinadas com um bloco de texto extra no final. Por exemplo, você pode assinar cada e-mail com suas informações de contato. Para ativar essa opção, selecione *Habilitar Assinatura* e decida se quer obter a assinatura a partir de um arquivo, de um campo de entrada ou da saída de um comando. Após concluir todas as suas configurações de identidade, confirme com *OK*.

As configurações em *Rede* decidem como o Kontact recebe e envia e-mail. Existem duas guias: uma para o envio e outra para o recebimento de mensagens. Muitas configurações variam de acordo com o sistema e a rede em que seu servidor de mensagens está localizado. Se você não tiver certeza sobre as configurações ou os itens a serem selecionados, consulte seu Provedor de Serviços de Internet ou o administrador do sistema.

Para criar caixas de saída de mensagens na guia *Envio*, clique em *Adicionar*. Escolha entre os tipos de transporte SMTP e sendmail. SMTP é a opção correta na maioria dos casos. Após essa seleção, será exibida uma janela na qual você pode digitar os dados do servidor SMTP. Forneça um nome e digite o endereço do servidor (como fornecido por seu Provedor de Serviços de Internet). Se o servidor requer que você se autentique, habilite *Servidor requer autenticação*. As configurações de segurança estão na guia *Segurança*, que é o local no qual você especifica o método de criptografia de sua preferência.

Selecione as configurações para o recebimento de e-mail na guia *Recebendo*. Use a opção *Adicionar* para criar uma conta nova. Escolha um dos diferentes métodos de recuperação de e-mail, como local (armazenado em formato Mbox ou Maildir), POP3 ou IMAP. Torne as configurações adequadas para o seu servidor.

12.3.2 Criando mensagens

Para criar novas mensagens, selecione *Mensagem → Nova Mensagem* ou clique no ícone correspondente na barra de ferramentas. Para enviar mensagens de diferentes contas de e-mail, selecione uma das identidades conforme descrito na Seção 12.3.1, “Configurando contas” (p 183). Em *Para*, digite um endereço de e-mail ou parte de um nome ou endereço no bloco de endereços. Se o Kontact puder fazer a correspondência entre aquilo que você digita e algo que esteja no bloco de endereços, será aberta uma lista de seleção. Clique no contato desejado ou complete a sua entrada se nenhuma delas corresponder. Para selecionar diretamente do bloco de endereços, clique no botão ..., ao lado do campo Endereço.

Para anexar arquivos à sua mensagem, clique no ícone em forma de clipe de papel e selecione o arquivo a ser anexado. Você também pode arrastar o arquivo da área de trabalho ou de outra pasta e soltá-lo na janela *Nova Mensagem* ou selecionar uma das opções do menu *Anexar*. Normalmente, o formato de um arquivo é reconhecido corretamente. Se o formato não for reconhecido, clique com o botão direito do mouse no ícone. No menu que aparece, selecione *Propriedades*. Defina o formato e o nome do arquivo na próxima caixa de diálogo e adicione uma descrição. Além disso, decida se o arquivo anexado deve ser assinado ou criptografado.

Ao terminar de redigir sua mensagem, envie-a imediatamente com *Mensagem* → *Enviar* ou mova a mensagem para a caixa de saída com *Mensagem* → *Fila*. Se você enviar o e-mail, a mensagem será copiada para `sent-mail` depois de ser enviada com sucesso. As mensagens movidas para `outbox` podem ser editadas ou apagadas.

12.3.3 E-mail criptografado e assinaturas

Para criptografar seus e-mails, primeiro gere um par de chaves como descrito no Capítulo 6, *Criptografia com KGpg* (p 103). Para configurar os detalhes do procedimento de criptografia, selecione *Configurações* → *Configurar KMail* → *Identidades* para especificar a identidade sob a qual enviará mensagens criptografadas e assinadas. Em seguida, pressione *Modificar*. Após confirmar com *OK*, a chave deverá ser exibida no campo correspondente. Feche a caixa de diálogo de configuração com *OK*.

12.3.4 Pastas

Pastas de mensagens ajudam a organizar as suas mensagens. Por padrão, elas estão localizadas no diretório `~/.kde/share/apps/kmail/mail`. Na primeira vez em que iniciar o KMail, o programa criará várias pastas. `inbox` é o local em que novas mensagens recebidas de um servidor são inicialmente armazenadas. `outbox` é usada para o armazenamento temporário de mensagens que estão na fila para serem enviadas. `sent-mail` é para cópias de mensagens enviadas. `trash` contém cópias de todos os e-mails apagados com Del ou *Editar* → *Apagar*. `drafts` é o local em que você pode gravar mensagens que não estão concluídas. Se você estiver usando IMAP, as pastas do IMAP serão relacionadas abaixo das pastas locais. Cada servidor de mensagens recebidas, por exemplo local ou IMAP, possui suas pastas na Lista de pastas.

Se você deseja organizar suas mensagens em pastas adicionais, crie novas pastas selecionando *Pasta → Nova Pasta*. Esse procedimento abre uma janela na qual você especifica o nome e o formato da nova pasta.

Clique com o botão direito do mouse na pasta para acessar um menu de contexto que oferece várias operações da pasta. Clique em *Expirar* para especificar a data de vencimento de mensagens lidas ou não lidas, o que deve acontecer com elas após o vencimento e se as mensagens expiradas devem ser apagadas ou movidas para uma pasta. Se você pretende usar a pasta para armazenar mensagens de uma lista de discussão, defina as opções necessárias em *Pasta → Gerenciamento de Lista de Discussão*.

Para mover uma ou várias mensagens de uma pasta para outra, realce as mensagens a serem movidas e pressione M ou selecione *Mensagem → Mover para*. Na lista de pastas exibida, selecione a pasta na qual você quer incluir as mensagens. As mensagens podem ser movidas se você arrastá-las da janela superior e soltá-las na pasta apropriada, na janela esquerda.

12.3.5 Filtros

Os filtros são um método conveniente de processar mensagens recebidas automaticamente. Eles usam aspectos da mensagem, como o remetente ou o tamanho, para mover a mensagem para determinadas pastas, para apagar mensagens indesejadas, retornar mensagens para o remetente ou realizar diversas outras ações.

Configurando um filtro

Para criar um filtro a partir do zero, selecione *Configurações → Configurar Filtros*. Para criar um filtro com base em uma mensagem existente, selecione a mensagem desejada na lista de cabeçalhos e, em seguida, selecione *Ferramentas → Criar Filtro* e os critérios do filtro desejado.

Selecione o método de correspondência para os critérios do filtro (todo ou qualquer). Em seguida, selecione os critérios que se aplicam somente às mensagens desejadas. Em *Ações de Filtro*, defina o que o filtro deve fazer com as mensagens que coincidirem com os critérios. *Opções Avançadas* oferece um controle de quando o filtro é aplicado e se filtros adicionais devem ser considerados para essas mensagens.

Aplicando filtros

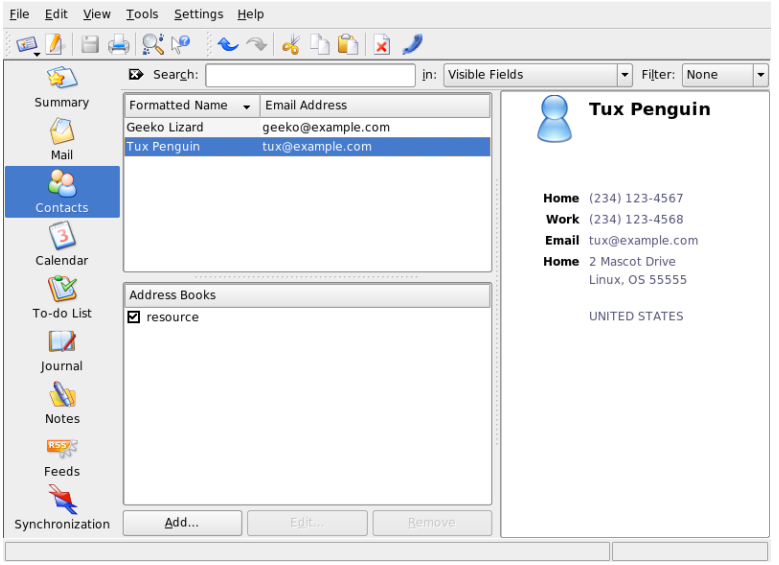
Os filtros são aplicados na ordem relacionada na caixa de diálogo acessada com *Configurações → Configurar Filtros*. Altere a ordem, selecionando um filtro e clicando nos botões de seta. Os filtros são aplicados somente em novas mensagens recebidas ou enviadas, como especificado nas opções avançadas do filtro. Para aplicar filtros em mensagens existentes, selecione as mensagens desejadas e *Mensagem → Aplicar Filtros*.

Caso os seus filtros não atuem conforme o esperado, monitore-os com *Ferramentas → Visualizador de Registro do Filtro*. Quando o registro estiver habilitado nessa caixa de diálogo, ela mostrará como as mensagens são processadas por seus filtros e podem ajudar a localizar o problema.

12.4 Contatos

O componente de contatos usa o KAddressBook. Configure-o com *Configurações → Configurar KAddressBook*. Para pesquisar um determinado contato, use a barra de pesquisa. Com *Filtro*, faça uma seleção para exibir somente os contatos de uma determinada categoria. Clique com o botão direito do mouse para abrir um menu no qual você seleciona uma variedade de opções, como o envio de informações de contato em um e-mail.

Figura 12.3 *O bloco de endereços do Kontact*



12.4.1 Adicionando contatos

Para que você, a partir de um e-mail, possa adicionar um contato com o nome e endereço de e-mail, clique com o botão direito do mouse no endereço no componente de e-mail e selecione *Abrir no Bloco de Endereços*. Para adicionar um novo contato sem usar um e-mail, selecione *Arquivo → Novo Contato* no componente de endereço. Os dois métodos abrem uma caixa de diálogo na qual você digita as informações sobre o contato.

Na guia *Geral*, digite as informações básicas do contato, como nome, endereço de e-mail e números de telefone. As categorias podem ser usadas para classificar os endereços. *Detalhes* contém mais informações específicas, como aniversário e nome do esposo.

Se o seu contato usar um programa de mensagem instantânea, você poderá adicionar essas identidades em *Endereço IM*. Se você fizer isso e o Kopete ou outro programa de bate-papo do KDE estiver sendo executado simultaneamente com o Kontact, exiba informações de status sobre essas identidades no Kontact. Em *Configurações de Criptografia*, digite os dados de criptografia do contato, como a chave pública.

Misc possui informações adicionais, como uma fotografia e o local das informações do tipo Livre/Ocupado do usuário. Use *Campos Personalizados* para adicionar suas próprias informações ao contato ou ao bloco de endereços.

Os contatos também podem ser importados em uma variedade de formatos. Use *Arquivo → Importar* e selecione o formato desejado. Em seguida, selecione o arquivo a ser importado.

12.4.2 Criando uma lista de distribuição

Se você envia mensagens de e-mail com freqüência para o mesmo grupo de pessoas, uma lista de distribuição permite que você armazene vários endereços de e-mail como o item de um único contato de forma que você não tenha que digitar cada nome individualmente em cada e-mail que envia para esse grupo. Primeiro, clique em *Configurações → Mostrar Barra de Extensão → Editor de Lista de Distribuição*. Na nova seção que aparece, clique em *Nova Lista*. Digite um nome para a lista e clique em *OK*. Adicione contatos à lista arrastando-os da lista de endereços e soltando-os na janela da lista de distribuição. Use essa lista como faria com um contato individual ao criar um e-mail.

12.4.3 Adicionando blocos de endereços

IMPORTANTE: Blocos de endereços de groupware

A melhor maneira de adicionar recursos de groupware é através do Assistente Groupware, uma ferramenta separada. Para usá-lo, feche o Kontact e, em seguida, execute `groupwarewizard` na linha de comando ou no grupo do Office do menu do KDE. Selecione o tipo de servidor, como SLOX, GroupWise ou Exchange, na lista oferecida e, em seguida, digite os dados do endereço e da autenticação. Em seguida, o assistente adiciona os recursos disponíveis ao Kontact.

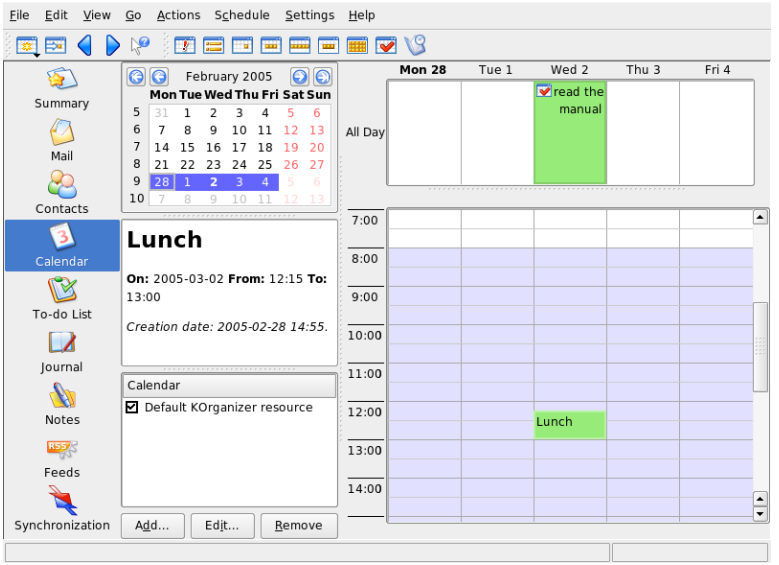
O Kontact pode acessar vários blocos de endereços, como alguns que estejam compartilhados e sejam oferecidos pelo Novell GroupWise ou por um servidor LDAP. Selecione *Configurações → Mostrar Barra de Extensão → Blocos de Endereços* para exibir os blocos de endereços atuais. Pressione *Adicionar* para adicionar um endereço e, em seguida, selecione o tipo e digite as informações necessárias.

As caixas de seleção em frente aos blocos mostram o status de ativação de cada bloco de endereço. Para impedir a exibição de um bloco sem apagá-lo, anule sua seleção. *Remover* apaga o bloco selecionado da lista.

12.5 Calendário

O Kontact usa o KOrganizer como seu componente de calendário. Para configurá-lo, use *Configurações → Configurar KOrganizer*. Com o calendário, digite compromissos e programe reuniões com outras pessoas. Se desejar, você pode ser lembrado de futuros eventos. Também pode importar, exportar e arquivar calendários com as opções em *Arquivo*.

Figura 12.4 *O calendário do Kontact*



12.5.1 Programando um evento

Adicione um novo evento ou reunião com *Ações → Novo Evento*. Digite os detalhes desejados. Em *Lembrete*, especifique o horário exato (minutos, horas ou dias de antecedência) no qual os participantes devem ser lembrados do evento. Se um evento for recorrente, especifique o intervalo adequado. Outra forma de criar um evento em

um ponto específico no calendário é clicar duas vezes no campo correspondente em uma das telas do calendário do programa. Esse procedimento abre a janela da mesma caixa de diálogo disponível pelo menu. Outra opção é selecionar o intervalo de tempo na tela Calendário e clicar com o botão direito do mouse.

Especifique os participantes de um evento, digitando seus dados manualmente na caixa de diálogo ou inserindo os dados a partir do bloco de endereços. Para digitar os dados manualmente, selecione *Novo*. Para importar os dados do bloco de endereços, clique em *Selecionar destinatário* e, em seguida, selecione as entradas correspondentes na caixa de diálogo. Para programar o evento com base na disponibilidade dos participantes, vá para *Livre/Ocupado* e clique em *Escolher Data*.

Use a guia *Recorrência* para configurar um evento que acontece regularmente. Os *Anexos* podem ser convenientes para vincular outras informações ao evento, como uma agenda para uma reunião.

12.5.2 Adicionando calendários

IMPORTANTE: Calendários de groupware

A melhor maneira de adicionar recursos de groupware é através do Assistente Groupware, uma ferramenta separada. Para usá-lo, feche o Kontact e, em seguida, execute `groupwarewizard` na linha de comando ou no grupo do Office do menu do KDE. Selecione o tipo de servidor, como SLOX, GroupWise ou Exchange, na lista oferecida e, em seguida, digite os dados do endereço e da autenticação. Em seguida, o assistente adiciona os recursos disponíveis ao Kontact.

O módulo do calendário pode se conectar a vários calendários simultaneamente. Isso é útil, por exemplo, para combinar um calendário pessoal com um organizacional. Para adicionar um novo calendário, clique em *Adicionar* e selecione o tipo de calendário. Complete os campos necessários.

As caixas de seleção em frente aos calendários mostram o status de ativação de cada um deles. Para impedir a exibição de um calendário sem apagá-lo, anule sua seleção. *Remover* apaga o calendário selecionado da lista.

12.6 Sincronizando dados com um dispositivo portátil

O Kontact foi desenvolvido de forma que os seus dados possam ser sincronizados com dispositivos portáteis, como um Palm. Veja informações sobre o status do KPilot no resumo. Consulte o Capítulo 13, *Sincronizando um computador portátil com o KPilot* (p 195) para obter informações sobre como configurar e usar o KPilot.

12.7 Kontact para usuários do GroupWise

Se você estiver habituado a trabalhar com o GroupWise, deverá ter poucos problemas para se adaptar ao Kontact. Os dois programas compartilham muitos conceitos e fornecem vários serviços iguais. Esta seção discute diferenças de terminologia consideráveis e fornece algumas dicas para ajudar os usuários do GroupWise a tirar o máximo de proveito do Kontact.

12.7.1 Diferenças de terminologia

A tabela a seguir relaciona algumas das diferenças principais de terminologia entre o Kontact e o GroupWise.

Tabela 12.1 *Diferenças de terminologia entre o Kontact e o GroupWise*

GroupWise	Kontact
Compromissos	Eventos
Ocupado	Livre/Ocupado
Notas	Entradas do Diário

GroupWise	Kontact
Itens publicados ou não publicados	Um evento sem participantes é publicado. Se houver participantes em um evento, este será um item enviado.
Tarefas	Pendências

12.7.2 Dicas para usuários do GroupWise

Esta seção contém dicas para ajudar os usuários do GroupWise a lidar com algumas diferenças entre o GroupWise e o Kontact.

Informações dos contatos

Você pode adicionar o GroupWise Messenger e contatos de e-mail às informações dos seus contatos do Kontact. Em seguida, você pode criar um e-mail ou abrir uma sessão de mensagens instantâneas com esse contato, clicando com o botão direito do mouse na tela Contatos.

Codificação de cores

É útil atribuir um código de cor a itens do GroupWise, bem como a itens de outras fontes. A codificação de cores facilita a exploração de e-mails, contatos e outras informações de itens de uma determinada fonte.

Convidando participantes para eventos

Diferentemente do GroupWise, o Kontact não o insere automaticamente como um participante dos eventos que você programa. Não se esqueça de enviar um convite para você.

12.8 Mais informações

O Kontact contém uma ajuda dele próprio e de seus vários componentes. Acesse esse recurso com *Ajuda* → *Manual do Kontact*. A página Web do projeto, http://www.kontact.org, também é informativa.

Sincronizando um computador portátil com o KPilot

13

O uso dos computadores portáteis está generalizado entre os usuários que precisam sempre carregar consigo programações, listas de afazeres e anotações. Muitas vezes, os usuários querem que os mesmos dados fiquem disponíveis tanto no desktop como no dispositivo portátil. É aí que entra o KPilot: trata-se de uma ferramenta para sincronizar dados em um dispositivo portátil com o dispositivo usado pelos aplicativos do KDE KAddressBook, KOrganizer e KNotes, que fazem parte do Kontact.

O principal objetivo do KPilot é permitir o compartilhamento de dados entre os aplicativos de um computador portátil e seus correspondentes do KDE. O KPilot vem com seu próprio visualizador de memorandos embutido, visualizador de endereços e instalador de arquivos, que não podem, entretanto, ser usados fora do ambiente do KPilot. Aplicativos independentes do KDE estão disponíveis para todas essas funções, exceto o instalador de arquivos.

Para a comunicação entre o dispositivo portátil e os diferentes programas do desktop, o KPilot conta com conduítes. O próprio KPilot é o programa que monitora todos os intercâmbios de dados entre os dois computadores. O uso de uma determinada função do dispositivo manual em seu desktop exige que o conduíte correspondente esteja habilitado e configurado. No geral, como esses conduítes são projetados para interagir com programas do KDE específicos, eles normalmente não podem ser usados com outros aplicativos de desktop.

O conduíte de sincronização de horário é especial porque não tem um programa visível ao usuário. Ele é ativado em segundo plano com cada operação de sincronização, porém somente deve ser habilitado em computadores que usam um servidor de horário de rede para corrigir seu próprio registro de tempo.

Quando uma sincronização é iniciada, os conduítes são ativados em seqüência para a realização da transferência de dados. Há dois métodos diferentes de sincronização: uma operação de HotSync somente sincroniza os dados para os quais conduítes tenham sido habilitados, ao passo que uma operação de backup realiza um backup completo de todos os dados armazenados no dispositivo portátil.

Alguns conduítes abrem um arquivo durante uma operação de sincronização, o que significa que o programa correspondente não deve estar em execução naquele momento. Em termos específicos, o KOrganizer não deve estar em execução durante uma operação de sincronização.

13.1 Conduítes usados pelo KPilot

Os conduítes usados pelo KPilot podem ser habilitados e configurados após a seleção de *Configurações → Configurar KPilot*. A seguir há uma lista de alguns conduítes importantes:

Bloco de Endereços
: Esse conduíte trata o intercâmbio de dados com o bloco de endereços do dispositivo portátil. O correspondente do KDE para o gerenciamento desses contatos é o KAddressBook. Inicie-o no menu principal ou com o comando `kaddressbook`.

KNotes/Memorandos
: Esse conduíte permite transferir anotações criadas com o KNotes para o aplicativo de memorandos do dispositivo portátil. Inicie o aplicativo do KDE no menu principal ou com o comando `knotes`.

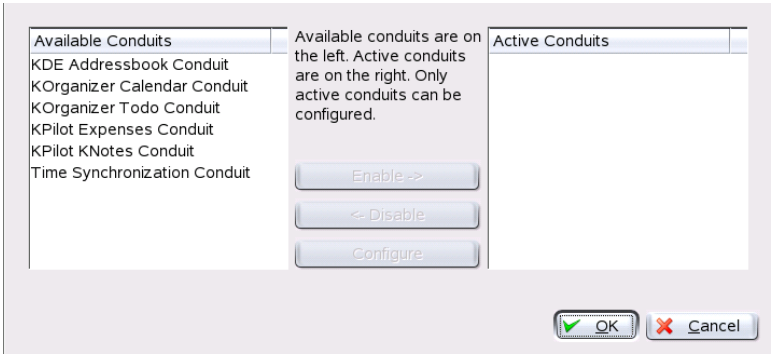
Calendário (KOrganizer)
: Esse conduíte é responsável pela sincronização dos compromissos (eventos) do dispositivo portátil. O equivalente no desktop é o KOrganizer.

Afazeres (KOrganizer)
: Esse conduíte é responsável pela sincronização dos afazeres. O equivalente no desktop é o KOrganizer.

Conduíte de Sincronização de Horário
: A habilitação desse conduíte ajusta o relógio do dispositivo portátil ao relógio do desktop durante cada operação de sincronização. Essa somente é uma boa idéia se

o próprio relógio do desktop for corrigido por um servidor de horário em intervalos razoavelmente freqüentes.

Figura 13.1 *Caixa de diálogo de configuração com os conduítes disponíveis*



13.2 Configurando a conexão do dispositivo portátil

Para poder usar o KPilot, primeiro configure a conexão com o computador portátil. A configuração depende do tipo de encaixe (unidade de acoplagem) usado com o dispositivo portátil. Há dois tipos de encaixe: Encaixes ou cabos USB e encaixes ou cabos seriais.

13.2.1 Configurando a conexão de dentro do KPilot

A maneira mais fácil de configurar a conexão é usando o assistente de configuração. Selecione *Configurações → Assistente de Configuração*para iniciar o assistente. No primeiro passo, digite seu nome de usuário e o nome do dispositivo ao qual o computador portátil está conectado. O assistente tenta detectá-los sozinho se você selecionar *Detectar Automaticamente o Dispositivo Portátil & Nome de Usuário*. Se a detecção automática falhar, consulte a Seção 13.2.2, “Criando um link /dev/pilot” (p 198).

Após confirmar com *Próximo*, o assistente solicita a especificação dos aplicativos que devem ser usados para a sincronização. Você pode escolher entre a suíte de aplicativos do KDE (padrão), Evolution e nenhum. Após selecionar, clique em *Concluir* para fechar a janela.

13.2.2 Criando um link /dev/pilot

A configuração da conexão com um encaixe portátil serial é diferente da conexão USB. Dependendo do encaixe usado, você pode ou não precisar criar um link simbólico chamado `/dev/pilot`.

USB
: Normalmente, um encaixe USB é detectado automaticamente, de modo que não deve haver a necessidade de criação do link simbólico mencionado.

Serial
: Com um encaixe serial, é necessário saber a qual porta serial ele é efetivamente conectado. Os dispositivos seriais recebem o nome de `/dev/ttyS?`, começando a partir de `/dev/ttyS0` para a primeira porta. Para configurar um encaixe conectado à primeira porta serial, digite o comando:

```
ln -s /dev/ttyS0 /dev/pilot
```

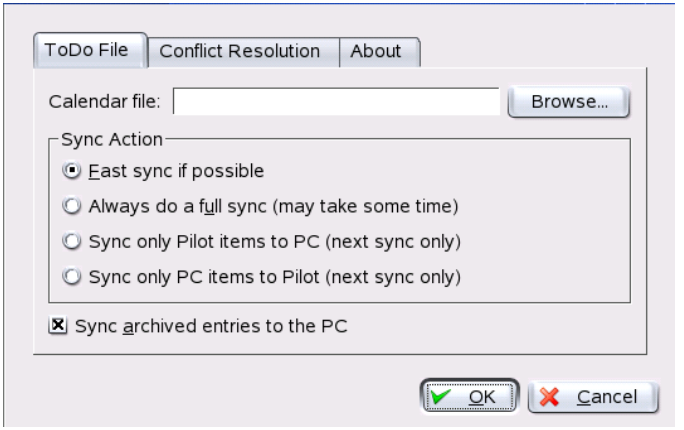
13.3 Configurando o conduíte do KAddressBook

Inicialmente, deve ser suficiente habilitar o conduíte do KAddressBook sem alterar nenhum valor predeterminado. Após a primeira sincronização dos dados, configure os detalhes: o que fazer em caso de conflitos, a forma como os bancos de dados de backup são gravados e como certos campos armazenados no dispositivo portátil devem ser atribuídos aos campos esperados pela KAddressBook.

13.4 Gerenciando itens de afazeres e eventos

Na área de trabalho do KDE, afazeres (tarefas) e eventos (compromissos) são gerenciados com o KOrganizer. Inicie o aplicativo no menu principal, com o comando `korganizer` ou como parte do Kontact. Após habilitar o calendário e o conduíte de afazeres do KPilot, defina algumas opções de configuração antes de usá-las.

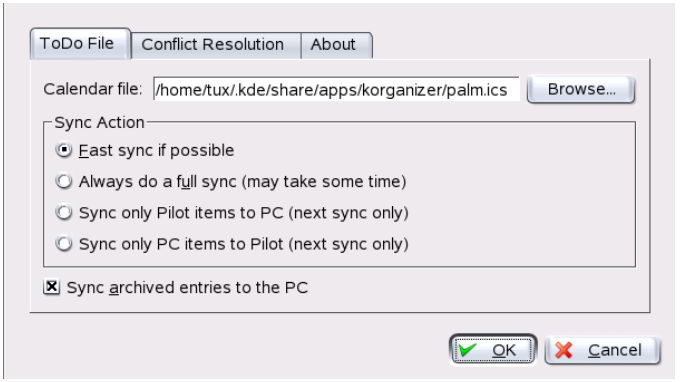
Figura 13.2 *Configuração do KPilot*



O KOrganizer armazena seus arquivos no diretório `~/.kde/share/apps/korganizer`. Entretanto, tendo em vista que o diretório `.kde/` começa com um ponto, ele pode não ser exibido pela caixa de diálogo de seleção de arquivos. Nesse caso, digite o caminho completo ou alterne explicitamente a exibição de arquivos ocultos (arquivos com ponto) na caixa de diálogo de seleção. O atalho padrão para isso é F8.

Após abrir o diretório `~/.kde/share/apps/korganizer`, selecione um arquivo que possa ser usado como arquivo de calendário pelo KOrganizer. Nesse exemplo, trata-se do arquivo `palm.ics`. No caso de um usuário chamado `tux`, o caminho e nome de arquivo completos seriam `/home/tux/.kde/share/apps/korganizer/palm.ics`, conforme mostra Figura 13.3, “Caixa de diálogo mostrando o caminho para um arquivo de calendário do KOrganizer” (p 200).

Figura 13.3 *Caixa de diálogo mostrando o caminho para um arquivo de calendário do KOrganizer*

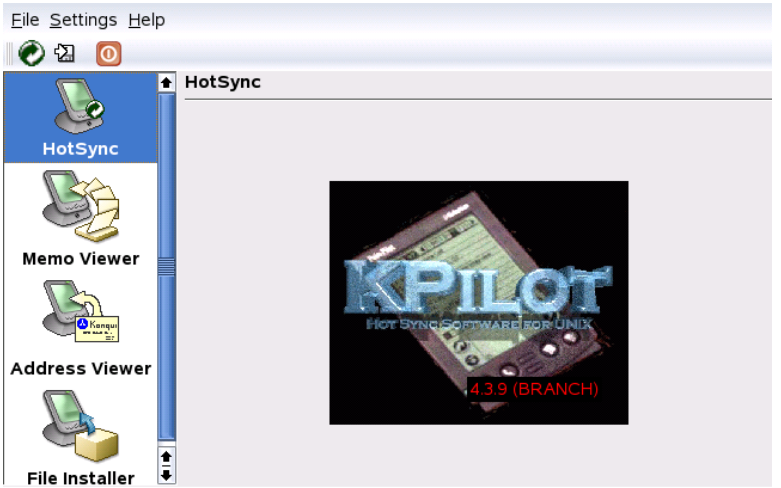


O KOrganizer não deve estar em execução quando estiverem sendo intercambiados dados com o dispositivo portátil. Do contrário, o KPilot não consegue realizar a operação de sincronização.

13.5 Trabalhando com o KPilot

A sincronização dos dados dos aplicativos do KDE com os dados do computador portátil é bastante fácil. Basta iniciar o KPilot e, em seguida, pressionar o botão HotSync no encaixe ou cabo para iniciar a operação de sincronização.

Figura 13.4 *Janela principal do KPilot*



13.5.1 Fazendo backup de dados do dispositivo portátil

Para fazer um backup completo, selecione *Arquivo → Backup*. O backup é realizado durante a próxima operação de sincronização. Depois disso, para alternar para o estado anterior, selecione *Arquivo → HotSync* no menu. Do contrário, o demorado backup completo será realizado novamente durante a próxima operação de sincronização.

Após um backup completo, todas as cópias dos programas e bancos de dados do computador portátil serão encontradas em `~/.kde/share/apps/kpilot/DBBackup/USERNAME`, em que *`USERNAME`* é o nome do usuário registrado no dispositivo da mapa.

Os dois visualizadores do KPilot embutidos podem ser usados para uma rápida consulta a endereços e memorandos, porém não foram projetados para fazer o gerenciamento de fato desses dados. Os aplicativos do KDE citados acima são bem mais adequados a essas tarefas.

13.5.2 Instalando programas no dispositivo portátil

O módulo *Instalador de Arquivos* é uma ferramenta interessante e útil para a instalação de programas portáteis. Esses programas normalmente possuem a extensão `.prc` e estão prontos para iniciar imediatamente após seu upload no dispositivo. Antes de usar esses programas de expansão, leia as respectivas licenças e também as instruções.

13.5.3 Sincronizando seus blocos de endereços e calendários

Para sincronizar seus calendários e endereços, use as ferramentas do KDE, MultiSynK. Inicie a ferramenta com o comando `multisynk`. Crie um par Konnector antes de sincronizar os dados. Vá até *Arquivo → Novo* e selecione seus Konnectors. Aprove com *Ok*.

O nome é listado na janela principal. Para sincronizar com um computador portátil, vá até *Arquivo → Sync*.

14 Usando o Beagle

Beagle é uma ferramenta de pesquisa que indexa o espaço de suas informações pessoais para ajudá-lo a encontrar o que você estiver procurando. Você pode usar o Beagle para encontrar documentos, e-mails, históricos da Web, conversas do Instant Messenger e ITC, códigos-fonte, imagens, arquivos de música, aplicativos e muito mais.

O Beagle suporta as seguintes origens de dados:

- Sistemas de arquivos
- Disparadores de aplicativos
- Bloco de endereços e correio do Evolution
- Registros de mensagens instantâneas do Gaim
- Páginas da Web do Firefox (conforme são exibidas)
- Agregadores RSS Blam e Liferea
- Anotações do Tomboy

Ele também suporta os seguintes formatos de arquivo:

- OpenOffice.org
- Microsoft Office (doc, ppt, xls)
- HTML

- PDF
- Imagens (jpeg, png)
- Áudio (mp3, ogg, flac)
- AbiWord
- Rich Text Format (rtf)
- Texinfo
- Páginas de manual
- Código-fonte (C, C++, C#, Fortran, Java, JavaScript, Pascal, Perl, PHP, Python)
- Texto simples

O Beagle indexa automaticamente tudo no diretório pessoal, mas você pode excluir certos arquivos ou diretórios. Ele também contém várias ferramentas que você pode usar para pesquisar os dados.

14.1 Indexando dados

O daemon do Beagle (`beagled`) executa automaticamente todas a indexação. Por padrão, todo o conteúdo do diretório pessoal é indexado. O Beagle detecta as mudanças feitas nesse diretório e reindexa os dados de forma adequada.

- Os arquivos são indexados imediatamente quando criados, são reindexados quando modificados e são eliminados do índice quando apagados.
- Os e-mails são indexados logo que recebidos.
- As conversas do IM são indexadas durante o bate-papo, uma linha por vez.

A indexação dos dados requer uma quantidade considerável de energia computacional, mas o daemon do Beagle tenta ser moderado o máximo possível. Ele contém um programador que trabalha para priorizar as tarefas e controlar o uso da CPU, com base no fato de você estar usando ativamente sua estação de trabalho.

14.1.1 Impedindo que arquivos e diretórios sejam indexados

Se você deseja impedir que um diretório e todos os seus subdiretórios sejam indexados, crie um arquivo vazio chamado `.noindex` e coloque-o no diretório. Você pode adicionar uma lista de arquivos e diretórios ao arquivo `.noindex` para impedir que esses arquivos e diretórios sejam indexados. Curingas são permitidos no arquivo `.noindex`.

Você também pode colocar um arquivo `.neverindex` no seu diretório pessoal com uma lista dos arquivos que nunca devem ser indexados. Curingas também são permitidos nesse arquivo. Use os mesmos curingas usados para `glob` (por exemplo, `f*le??.txt`). Também é possível usar expressões regulares mais eficientes adicionando uma barra normal antes e depois do padrão, `/file.*.txt/`). Para obter mais informações, consulte o site glob-UNIX na Web (http://docs.python.org/lib/module-glob.html).

14.1.2 Indexando manualmente

O Beagle tem um sistema eficiente que determina quando os arquivos devem ser indexados, além de tentar não interferir nos outros aplicativos em execução. Ele sincroniza intencionalmente sua indexação com base na carga e na inatividade do sistema, de modo a não afetar negativamente a utilização da área de trabalho. Contudo, se você deseja indexar imediatamente o diretório pessoal, digite o seguinte comando em uma janela de terminal antes de executar o Beagle:

```
export BEAGLE_EXERCISE_THE_DOG=1
```

14.1.3 Verificando o status do índice

O Beagle contém os seguintes comandos para que você possa ver o status atual da indexação:

`beagle-index-info`
: Exibe quantos documentos foram indexados e que tipo de documentos foram indexados.

`beagle-status`
Exibe o trabalho que o daemon do Beagle está realizando (continuamente).

14.2 Pesquisando dados

O Beagle oferece as seguintes ferramentas para que os dados indexados sejam pesquisados.

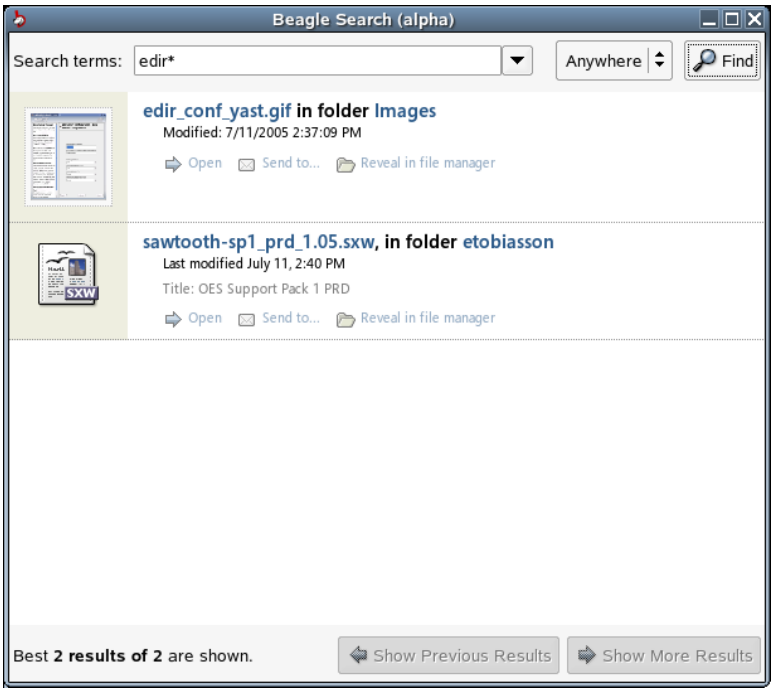
14.2.1 Best

Best (Bleeding Edge Search Tool) é uma ferramenta gráfica que pesquisa as informações indexadas. Ela não consulta o índice diretamente; em vez disso, passa os termos da pesquisa ao daemon do Beagle, que envia as correspondências encontradas de volta ao Best. Em seguida, o Best exibe os resultados e permite a execução de ações nos objetos correspondentes.

Para abrir o Best no KDE, clique em *Menu K → Sistema → Sistema de Arquivos → Pesquisa via Beagle*. No GNOME, clique em *Aplicativos → Sistema → Sistema de Arquivos → Pesquisa via Beagle*.

Para usar o Best, basta digitar o texto da pesquisa na caixa de entrada na parte superior e pressionar Enter ou clicar em *Localizar*. O Best consulta os arquivos indexados e retorna os resultados.

Figura 14.1 *Pesquisa via Beagle*



Você pode usar a lista de resultados para abrir um arquivo ou enviá-lo por e-mail, enviar uma mensagem instantânea, repetir em um arquivo, encaminhar um arquivo ou exibi-lo no gerenciador de arquivos. As opções disponíveis para cada arquivo dependem de seu tipo.

Você também pode usar *Anywhere* para limitar a pesquisa a arquivos de um local específico, como seu bloco de endereços ou páginas da Web, ou para exibir somente um tipo específico de arquivo na lista de resultados.

14.2.2 beagle-query

O Beagle tem uma ferramenta de linha de comando que pode ser usada para pesquisar o índice do Beagle. Para usar essa ferramenta, digite o seguinte comando em uma janela de terminal:

```
beagle-query search
```

Substitua *search* pelo texto a ser localizado, e a ferramenta beagle-query retornará os resultados. Você pode usar curingas com esse comando.

Use `beagle-query --verbose` *search* para exibir informações detalhadas sobre os resultados da pesquisa.

Parte V Gráficos

15 Câmeras digitais e Linux

Se você tiver as ferramentas certas, o gerenciamento das fotos da sua câmera poderá ser divertido. O Linux oferece diversos utilitários práticos para a classificação e organização de fotografias. Entre eles estão o gphoto2, o Konqueror, o Digikam e o f-spot.

Uma lista abrangente de câmeras suportadas está disponível em `http://www.gphoto.org/proj/libgphoto2/support.php`. Se o gphoto2 estiver instalado, recupere a lista com o comando `gphoto2 --list-cameras`. Informações sobre os comandos disponíveis podem ser obtidas com `gphoto2 --help`.

DICA: Câmeras não suportadas

Se você não encontrar sua câmera na lista do gphoto, não se preocupe. É bem provável que o suporte à sua câmera seja o mesmo dado a dispositivos de armazenamento em massa USB. Mais informações podem ser encontradas em Seção 15.2, “Acessando a câmera” (p 212).

15.1 Conectando a câmera

A forma mais rápida e conveniente de conectar câmeras digitais ao computador é o USB, contanto que este seja suportado pelo kernel, pela câmera e pelo computador. O kernel SUSE padrão oferece esse suporte. Um cabo adequado também é necessário.

Basta conectar a câmera à porta USB e ligá-la. Talvez seja necessário usar um modo de transferência especial na câmera. Sobre esse procedimento, consulte o manual da câmera digital.

15.2 Acessando a câmera

Existem três possibilidades de acesso às fotografias da câmera, a depender da câmera e do protocolo suportado por ela. Em geral, é usado o armazenamento em massa USB, que é tratado pelo sistema hotplug, ou o protocolo PTP (também conhecido como PictBridge). Alguns modelos de câmera não funcionam com nenhum dos dois protocolos. Para dar suporte a esses modelos, o gphoto2 vem com drivers específicos.

Tudo fica mais fácil se a sua câmera vier com suporte para armazenamento em massa USB. Leia a documentação da sua câmera se não tiver certeza dessa possibilidade. Algumas dão suporte a dois protocolos, como o PTP e o armazenamento em massa USB. Infelizmente, também existem algumas que se comunicam com um protocolo proprietário, o que pode complicar as tarefas. Se sua câmera não oferecer suporte ao armazenamento em massa USB ou ao PTP, as descrições a seguir não funcionarão. Experimente usar o comando `gphoto2 --list-cameras` e as informações contidas em `http://www.gphoto.org/`.

Se a sua câmera puder ser comutada para um dispositivo de armazenamento em massa USB, selecione essa opção. Depois de conectada à porta USB do computador e ligada, ela será detectada pelo sistema hotplug. Desse modo, o dispositivo é montado automaticamente, para que seu acesso fique fácil. A área de trabalho do KDE exibe um ícone de câmera quando a montagem é bem-sucedida.

Depois de montar a câmera com êxito, você verá um novo diretório em `/media`, começando com `usb` e vários números. Cada fornecedor e produto tem um número, dessa forma, o nome será o mesmo quando você conectar um dispositivo ao seu computador. Dependendo do que foi conectado ao barramento USB, você encontrará entradas diferentes. O único problema restante é encontrar a entrada correta para a câmera. Tente listar um destes diretórios (`DCIM/`*`xxx`*) para ver o que acontece. Como cada câmera possui uma estrutura em árvore diferente, não existe uma regra geral. Se houver arquivos JPEG em um diretório, provavelmente você o encontrou.

Depois de encontrar o diretório correto, você poderá copiar, mover ou apagar os arquivos da câmera com um gerenciador de arquivos, como o Konqueror, ou com simples

comandos de shell (consulte Seção 27.3, “Comandos importantes do Linux” (p 420) e a *Referência*).

15.3 Usando o Konqueror

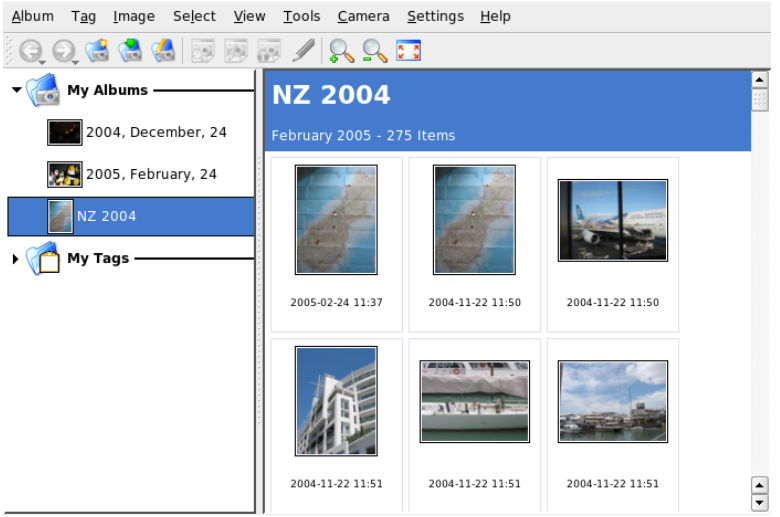
Os usuários do KDE podem acessar facilmente câmeras digitais por meio da conhecida interface do Konqueror. Conecte sua câmera à porta USB. Um ícone de câmera deve aparecer na área de trabalho. Clique nele para abrir a câmera no Konqueror. A câmera também poderá ser acessada digitando-se o URL `camera:/` no Konqueror. Navegue pela estrutura de diretórios da câmera até que os arquivos sejam exibidos. Use os recursos normais de gerenciamento de arquivos do Konqueror para copiar os arquivos conforme desejado. Para obter mais informações sobre como usar o Konqueror, consulte Capítulo 3, *Browser da Web Konqueror* (p 75).

15.4 Usando o Digikam

O Digikam é um programa KDE para download de fotografias de câmeras digitais. Na primeira vez em que é executado, o Digikam pergunta onde o álbum de fotos deve ser armazenado. Se você digitar um diretório que já contém uma coleção de fotografias, o Digikam tratará cada subpasta como um álbum.

Na inicialização, o Digikam apresenta uma janela com duas seções: seus álbuns são exibidos à esquerda e as fotografias do álbum atual são exibidas à direita. Consulte a Figura 15.1, “Janela principal do Digikam” (p 214).

Figura 15.1 *Janela principal do Digikam*



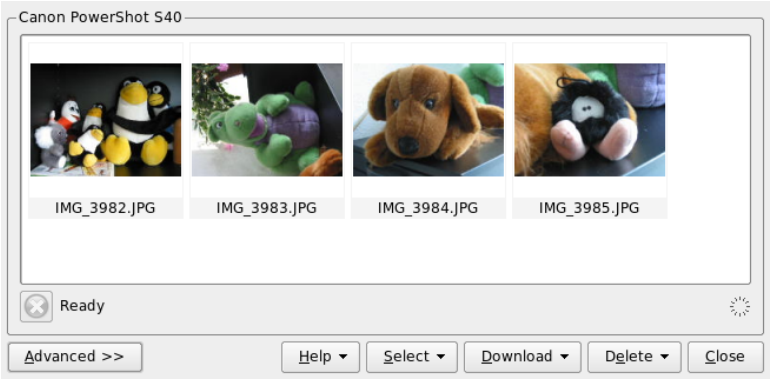
15.4.1 Configurando a câmera

Para configurar uma câmera no Digikam, selecione *Câmera → Adicionar Câmera*. Primeiro, tente detectar automaticamente a câmera com a opção *Detecção Automática*. Se isso não funcionar, percorra a lista e selecione seu modelo com *Adicionar*. Se seu modelo de câmera não estiver incluído na lista, use um modelo mais antigo ou use a *câmera de armazenamento em massa USB/IEEE*. Confirme com *OK*.

15.4.2 Fazendo download de fotos da câmera

Após a correta configuração da câmera, conecte-se a ela com o menu *Câmera* e o nome atribuído na caixa de diálogo a partir de Seção 15.4.1, “Configurando a câmera” (p 214). O Digikam abre uma janela e inicia o download de miniaturas e as exibe como em Figura 15.2, “Fazendo download de fotos da câmera” (p 215). Clique o botão direito do mouse em uma imagem para abrir um menu popup com as opções *Ver*, exibir algumas *Propriedades* ou *Informações EXIF*, *Fazer Download* ou *Apagar* a imagem. Em *Avançado*, selecione as opções de renomeação e e como trabalhar com as informações (EXIF) fornecidas pela câmera.

Figura 15.2 *Fazendo download de fotos da câmera*



As opções de renomeação podem ser bastante práticas se a câmera não usar nomes de arquivo expressivos. Você pode deixar que o Digikam renomeie as fotografias automaticamente. Dê um prefixo exclusivo e, opcionalmente, uma data, horário ou número de seqüência. O Digikam faz o resto.

Selecione todas as fotografias para download na câmera pressionando o botão esquerdo do mouse ou clicando em cada fotografia com a tecla Ctrl pressionada. As fotografias selecionadas aparecerão com cores invertidas. Clique em *Fazer Download*. Selecione o destino na lista ou crie um novo álbum com *Novo Álbum*. Essa opção sugere automaticamente um nome de arquivo com a data atual. Confirme com *OK* para iniciar o processo de download.

15.4.3 Obtendo informações

Não é difícil obter informações sobre a fotografia. Um breve resumo é exibido como uma dica de ferramenta quando você aponta o cursor do mouse para a miniatura. Para obter informações mais detalhadas, clique o botão direito do mouse na fotografia e selecione *Propriedades* no menu. Você verá uma caixa de diálogo com três guias: *Geral*, *EXIF* e *Histograma*.

A guia *Geral* lista nome, tipo, proprietário e outras informações básicas. A parte mais interessante é a guia *EXIF*. A câmera armazena alguns metadados para cada fotografia. O Digikam lê essas propriedades e as exibe nessa lista. Encontre o tempo de exposição, as dimensões em pixel etc. Para obter mais informações sobre a entrada selecionada na

lista, pressione Shift + F1. É exibida uma pequena dica de ferramenta. A última guia, *Histograma*, exibe informações estatísticas.

15.4.4 Gerenciando álbuns

O Digikam insere uma pasta chamada *Meus Álbuns* por padrão, que coleta todas as suas fotografias. Essas fotografias podem posteriormente ser armazenadas em subpastas. Os álbuns podem ser classificados pelo layout de diretório, pelo nome da coleção definido nas propriedades do álbum ou pela data de criação dos álbuns (essa data também pode ser mudada nas propriedades de cada álbum).

Algumas possibilidades para criar um novo álbum:

- Fazer o upload de novas fotografias da câmera
- Criar um novo álbum clicando no botão *Novo Álbum*, na barra de ferramentas
- Importar uma pasta de fotografias existente do disco rígido (selecione *Álbum → Importar → Importar Pastas*)
- Clicar o botão direito do mouse em *Importar Pastas* e selecionar *Novo Álbum*

Depois que você cria um álbum no modo que preferir, uma caixa de diálogo é exibida. Dê um título ao álbum. Opcionalmente, escolha uma coleção, insira comentários e selecione uma data para o álbum. Uma coleção é uma forma de organizar seus álbuns usando um rótulo comum. Esse rótulo é usado quando você seleciona *Ver → Ordenar Álbuns → Por Coleção*. O comentário é exibido no banner na parte superior da janela principal. A data do álbum é usada quando você seleciona *Ver → Álbuns → Por Data*.

O Digikam usa a primeira fotografia do álbum como o ícone de visualização na lista *Meus Álbuns*. Para selecionar outro ícone, clique o botão direito do mouse na respectiva fotografia e selecione *Definir como Miniatura do Álbum* no menu de contexto.

15.4.5 Gerenciando tags

Às vezes, o gerenciamento de uma grande quantidade de fotografias em diferentes álbuns pode ser uma tarefa complexa. Para organizar fotografias avulsas, o Digikam oferece o sistema *Minha Tag*.

Por exemplo, você fotografou seu amigo John em diferentes momentos e deseja coletar todas as imagens, independentemente do álbum onde estejam. Esse recurso permite que você encontre todas as fotografias com bastante facilidade. Primeiro, crie uma nova tag clicando em *Minhas Tags → Pessoas*. No menu de contexto, selecione *Nova Tag*. Na caixa de diálogo que aparece, digite *John* como título e, opcionalmente, defina um ícone. Confirme com *OK*.

Depois de criar a tag, atribua-a às imagens desejadas. Vá para cada álbum e selecione as respectivas fotografias. Clique o botão direito do mouse e escolha *Atribuir Tag → Pessoas → John* no menu exibido. Outra opção é arrastar as fotografias até o nome da tag em *MinhasTags* e soltá-las. Repita o procedimento com os outros álbuns conforme a necessidade. Para exibir todas as imagens, clique em *Minhas Tags → Pessoas → John*. Você pode atribuir mais de uma tag a cada fotografia.

A edição de tags e comentários pode ser tediosa. Para simplificar essa tarefa, clique o botão direito do mouse em uma fotografia e selecione *Editar Comentários e Tags*. Essa ação abre uma caixa de diálogo com uma visualização, um campo de comentários e uma lista de tags. Nessa caixa, você pode inserir todos os tags necessários e adicionar um comentário. Navegue no álbum usando *Avançar* e *Voltar*. Armazene suas mudanças com *Aplicar* e para sair use *OK*.

15.4.6 Exportando coleções de imagens

O Digikam oferece diversas opções de exportação úteis para o arquivamento e a publicação de coleções de imagens pessoais. Ele oferece arquivamento em CD ou DVD (com o aplicativo k3b), exportação em HTML e exportação para uma galeria remota.

Para gravar sua coleção de imagens em CD ou DVD, proceda da seguinte forma:

1. Selecione *Arquivo → Exportar → Arquivar em CD/DVD*.

2. Faça ajustes na caixa de diálogo *Criar Arquivo de CD/DVD* usando os diversos submenus. Em seguida, clique em *OK* para iniciar o processo de gravação.

   a. *Seleção*: Para determinar que parte da sua coleção deve ser arquivada, selecione álbuns e tags.

   b. *Interface HTML*: Decida se a coleção de imagens deve ficar acessível via interface HTML e se a funcionalidade de execução automática deve ser

adicionada ao arquivo de CD/DVD. Defina um título para a seleção e as propriedades de imagem, fonte e segundo plano.

c *Descritor do Volume de Mídia*: Mude as configurações da descrição de volume se necessário.

d *Gravação de Mídia*: Ajuste as opções de gravação conforme necessário.

Para criar uma exportação em HTML da sua coleção de imagens, proceda da seguinte maneira:

1 Selecione *Arquivo → Exportar → Exportação HTML*.

2 Use os diversos submenus para ajustar as configurações em *Criar Galerias de Imagens* às suas necessidades. Ao terminar, clique em *OK* para iniciar a criação da galeria.

a *Seleção*: Para determinar que parte da sua coleção deve ser arquivada, selecione álbuns e tags.

b *Aparência*: Defina o título e a aparência da galeria HTML.

c *Álbum*: Determine a localização da galeria no disco, assim como o tamanho, a compactação e o formato das imagens, e a quantidade de metadados exibida na galeria resultante.

d *Miniaturas*: Assim como as imagens de destino, especifique o tamanho, a compactação e o tipo de arquivo das miniaturas usadas na navegação da galeria.

Para exportar a coleção para uma galeria de imagens externa na Internet, proceda da seguinte forma:

1 Obtenha uma conta de um site externo que abrigue a galeria.

2 Selecione *Arquivo → Exportar → Exportar para Galeria Remota* e forneça o URL, o nome de usuário e a senha para o site externo quando for solicitado.

O Digikam estabelece uma conexão com o site especificado e abre uma nova janela chamada *Exportação de Galeria*.

3 Determine a localização do novo álbum no interior da galeria.

4 Clique em *Novo Álbum* e forneça as informações solicitadas pelo Digikam.

5 Para fazer o upload das imagens para o novo álbum, use *Adicionar Fotos*.

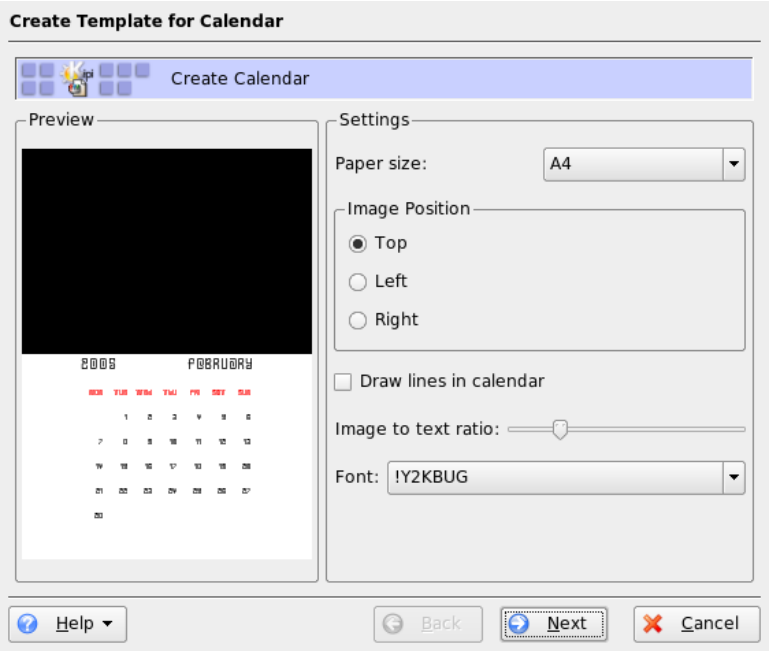
15.4.7 Ferramentas úteis

O Digikam oferece diversas ferramentas para simplificar algumas tarefas. Elas podem ser encontradas no menu *Ferramentas*. A seguir há uma pequena seleção das ferramentas disponíveis.

Criando um calendário

Se você quiser agradar alguém, um calendário personalizado pode ser um bom presente. Vá para *Ferramentas* → *Criar Calendário*, será aberto um assistente como esse em Figura 15.3, “Criando um modelo de calendário” (p 220).

Figura 15.3 *Criando um modelo de calendário*



Personalize as configurações (tamanho do papel, posição da imagem, fonte etc.) e confirme com *Próximo*. Agora é possível digitar o ano e selecionar as imagens a serem usadas. Depois de clicar em *Próximo* novamente, você verá um resumo. O último botão *Próximo* abre a caixa de diálogo da Impressora KDE. Nessa caixa, você pode escolher visualizar o calendário, gravá-lo no formato PDF ou imprimi-lo.

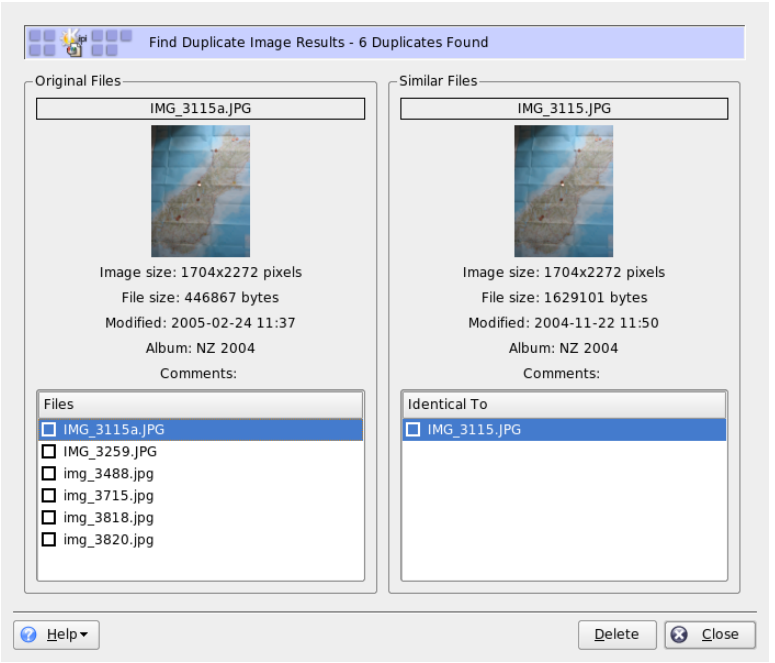
Procurando fotografias duplicadas

Às vezes, você tira várias fotos de cenas semelhantes e deseja manter apenas as melhores. Essa é a tarefa perfeita para o plug-in *Procurar Duplicata*.

Vá para *Ferramentas → Procurar Imagens Duplicadas*. Selecione os álbuns ou tags a serem usados. Em *Método e Cache*, escolha o método de pesquisa: um método mais preciso ou um método mais rápido. Depois que você confirma com *OK*, o Digikam prossegue com a investigação.

Se encontrar duplicatas, ele exibe o resultado em uma janela semelhante a Figura 15.4, “Resultados da busca” (p 221). Para selecionar as imagens a serem apagadas, ative as caixas de seleção desejadas e clique em *Apagar*. Para sair da janela, clique em *Fechar*.

Figura 15.4 *Resultados da busca*



Processos em lote

O Digikam também oferece alguns processos em lote que realizam uma tarefa específica em diversos arquivos. Essas tarefas podem ser renomeações, conversões, redimensionamentos e muitas outras. Esses processos estão localizados em *Ferramentas → Processos em Lote*.

15.4.8 Visualização e edição básica de imagens com o Digikam

O Digikam vem com seu próprio programa enxuto de visualização e edição de imagens. Ele abre automaticamente quando você clica duas vezes na miniatura de uma imagem.

Use essa ferramenta para fazer edições básicas nas imagens recém-baixadas da sua câmera. Você pode cortar, girar ou inverter a imagem, fazer ajustes básicos de cor, aplicar diversos filtros coloridos (por exemplo, exportar uma imagem colorida para preto e branco) e reduzir com eficiência olhos vermelhos em retratos.

Os menus mais importantes são:

Imagem
: Use *Editar Comentários e Tags* para digitar comentários para uma determinada imagem e para atribuir uma tag (categoria) a essa imagem. *Propriedades* abre uma janela com três guias contendo informações gerais, informações EXIF e o histograma da imagem.

Corrigir
: Esse menu contém algumas das funções de edição mais necessárias na fotografia digital. *Cores* conduz a um submenu onde você pode modificar todas as configurações básicas de cor. Também é possível aumentar ou reduzir a nitidez da imagem inteira ou de uma parte selecionada da imagem. Para reduzir o efeito de olhos vermelhos em um retrato, faça uma seleção preliminar da região do olho clicando e segurando o ponteiro esquerdo do mouse. Expanda gradualmente a seleção, escolha *Redução de Olho Vermelho* e selecione redução fraca ou forte dependendo da seleção feita (a área inteira ou apenas os olhos).

Transformar
: O menu *Transformar* oferece as funções de corte, giro, inversão e redimensionamento. Você também pode usar a opção *Corte de Proporção* para produzir cortes com uma proporção fixa.

Filtros
: Se você precisar transformar suas fotos coloridas em fotos em preto e branco e desejar dar um aspecto de envelhecimento a elas, verifique o menu *Filtros* e escolha uma entre as diversas opções de exportação.

Uma descrição mais detalhada dessa ferramenta pode ser encontrada na ajuda online do Digikam em *Editor de Imagens digiKam*, que pode ser acessado por meio do botão *Ajuda* na barra de menus do Digikam.

DICA: Processamento avançado de imagens

A edição profissional de imagens pode ser feita com o GIMP. Mais informações sobre o GIMP podem ser encontradas em Capítulo 17, *Manipulando gráficos com o GIMP* (p 241).

15.5 Usando o f-spot

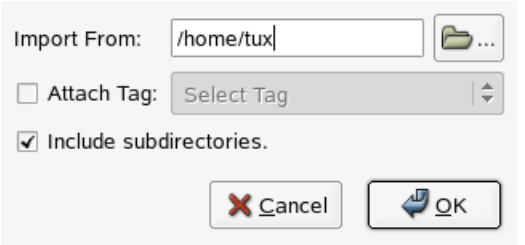
O f-spot é uma ferramenta de gerenciamento para a sua coleção de imagens digitais adaptada à área de trabalho do GNOME. Ela permite atribuir diferentes tags às imagens a fim de categorizá-las e oferece uma variedade de excelentes opções para edição de imagens.

A primeira vez que executar o f-spot, informe à ferramenta onde encontrar as imagens a serem importadas para a sua coleção do f-spot. Se você já tiver uma coleção de imagens armazenada no disco rígido, digite o caminho do respectivo diretório e, opcionalmente, inclua subpastas. O f-spot importa essas imagens para o banco de dados.

DICA: Marcando imagens na importação

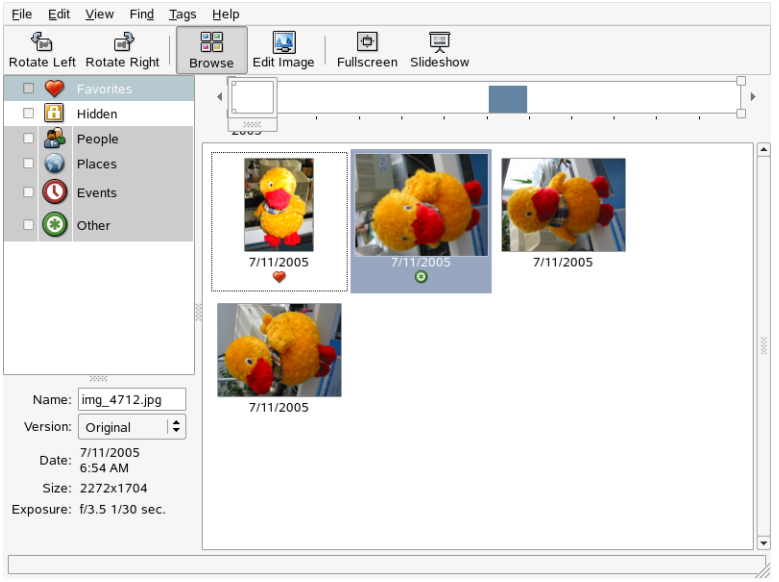
Se todas as imagens sendo importadas pertencerem à mesma categoria, você poderá anexar a tag apropriada na importação. Selecione *Anexar Tag* e escolha a tag correspondente no menu suspenso.

Figura 15.5 *Importando imagens para o f-spot*



A janela principal do f-spot está dividida em três áreas principais. Categorias, tags e informações detalhadas sobre as imagens selecionadas são exibidas em uma barra lateral à esquerda, enquanto a área direita da janela mostra uma miniatura de todas as imagens com a categoria ou a tag selecionada ou, se nada tiver sido selecionado, a coleção inteira.

Figura 15.6 *Janela principal do f-spot*



A barra de menus localizada na parte superior da janela permite acessar os menus principais. A barra de ferramentas na parte inferior oferece diversas funções diferentes representadas pelo ícone correspondente:

Girar para a Esquerda ou para a Direita
: Use esse atalho para mudar a orientação de uma imagem.

Pesquisar
: O modo *Pesquisar* permite exibir e pesquisar a coleção inteira ou subconjuntos com tags. Também é possível usar a linha de tempo para pesquisar imagens por data de criação.

Editar Imagem
Esse modo permite selecionar uma imagem e fazer processamentos básicos. Detalhes estão disponíveis em Seção 15.5.6, “Processamento básico de imagens com o f-spot” (p 230).

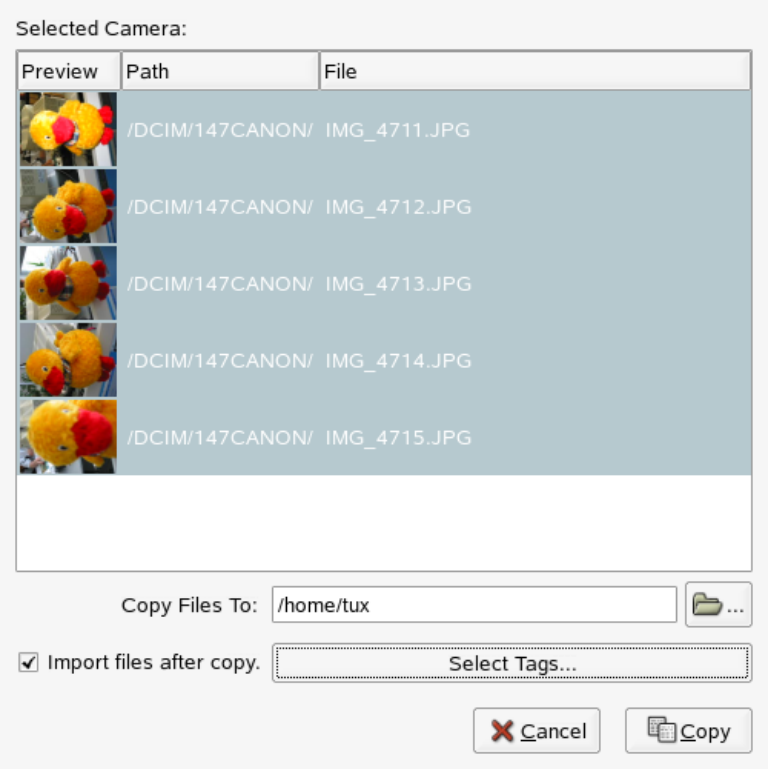
Tela Cheia
Alterne para o modo de exibição de tela cheia.

Show de Slides
Inicie uma apresentação de slides.

15.5.1 Fazendo download de fotos da câmera

Importe novas imagens da câmera digital conectada à porta USB do computador usando *Arquivo → Importar da Câmera*. A detecção do tipo de câmera é automática.

Figura 15.7 *Importar da câmera*



O f-spot inicia uma janela de visualização exibindo todas as imagens disponíveis para download da câmera. Os arquivos são copiados para o diretório de destino especificado por meio de *Copiar Arquivos para*. Se a opção *Importar arquivos depois de copiar* tiver sido selecionada, todas as imagens copiadas da câmera serão automaticamente importadas para o banco de dados do f-spot. A marcação com tags pode ser feita na importação, se você selecionar a tag apropriada com *Selecionar Tags*. Se não quiser importar todas as imagens da câmera para o banco de dados, basta anular a seleção das imagens indesejadas na janela de visualização.

15.5.2 Obtendo informações

Uma vez selecionada uma imagem, algumas informações estatísticas básicas sobre ela são exibidas na porção inferior esquerda da janela. Essas informações incluem o nome

do arquivo, sua versão (cópia ou imagem original), a data de criação, o tamanho e a exposição usada para criar a imagem. Exiba os dados EXIF associados ao arquivo de imagem usando *Ver → Dados EXIF*.

15.5.3 Gerenciando tags

Use tags para categorizar qualquer uma das suas imagens e criar subconjuntos gerenciáveis da coleção. Por exemplo, se desejar fazer algum tipo de ordenamento na sua coleção de retratos de pessoas queridas, proceda da seguinte forma:

1. Selecione o modo *Pesquisar* do f-spot.

2. No frame esquerdo da janela do f-spot, selecione a categoria *Pessoas*, clique o botão direito do mouse nela e escolha *(Criar Nova Tag)* Assim, os novos tags são exibidos como subcategorias da categoria *Pessoas*:

   a. Crie uma nova tag chamado `Amigos`.

   b. Crie uma nova tag chamado `Família`.

3. Agora, associe tags a imagens ou grupos de imagens selecionadas. Clique o botão direito em uma imagem, escolha *Anexar Tag* e selecione a tag apropriada para a imagem. Para associar uma tag a um grupo de imagens, clique na primeira imagem, pressione a tecla Shift e selecione as outras sem soltar a tecla Shift. Clique o botão direito do mouse no menu de tags e selecione a categoria correspondente.

Após a categorização das imagens, você poderá pesquisar sua coleção por tags. Basta procurar por *Pessoas → Família* e a coleção exibida será limitada às imagens com a tag `Família`. A pesquisa da coleção por tag também é possível por meio de *Procurar → Procurar por Tag*. O resultado da pesquisa é exibido na janela de visão geral de miniaturas.

A remoção de tags de imagens avulsas ou de grupos de imagens funciona do mesmo modo que a sua anexação. As funções de edição de tags também podem ser acessadas por meio do menu *Tags*, na barra de menus superior.

15.5.4 Pesquisar e Encontrar

Conforme mencionado em Seção 15.5.3, “Gerenciando tags” (p 227), os tags podem ser usados como um meio para se encontrar certas imagens. Outro método, exclusivo do f-spot, é usar a *Linha de Tempo* situada abaixo da barra de ferramentas. Arrastando o pequeno frame ao longo dessa linha do tempo, você limita as imagens exibidas na visão geral de miniaturas às imagens escolhidas no frame de tempo selecionado. O f-spot inicia com uma linha de tempo padrão criteriosamente escolhida, mas esse intervalo pode ser editado movendo os controles deslizantes para as extremidades direita e esquerda da linha de tempo.

15.5.5 Exportando coleções de imagens

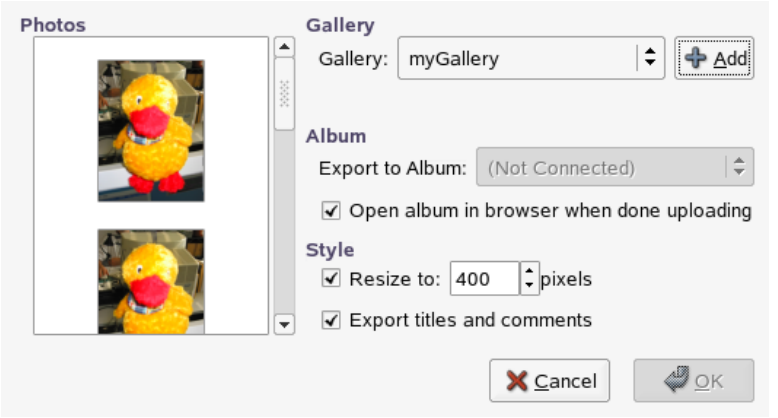
O f-spot oferece uma variedade de funções de exportação para as suas coleções em *Arquivo → Exportar*. É provável que as funções mais usadas sejam *Exportar para Galeria da Web* e *Exportar para CD*.

Para exportar uma seleção de imagens para uma galeria na Web, proceda da seguinte maneira:

1. Selecione as imagens a serem exportadas.

2. Clique em *Arquivo → Exportar → Exportar para Galeria da Web* e selecione uma galeria para a qual exportar as imagens ou adicione uma nova. O f-spot estabelece uma conexão com o local indicado como galeria da Web. Selecione o álbum para o qual exportar as imagens e decida se deseja dimensionar as imagens automaticamente e exportar títulos e comentários.

Figura 15.8 *Exportando imagens para uma galeria da Web*



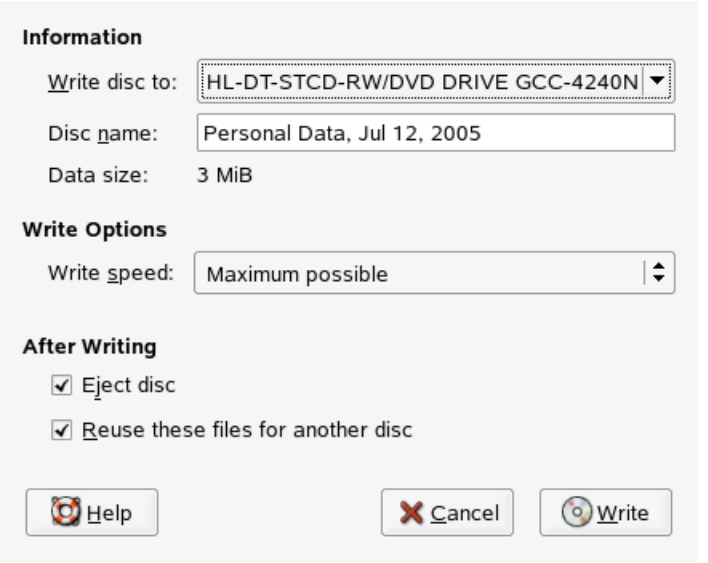
Para exportar uma seleção de imagens para um CD, proceda da seguinte maneira:

1. Selecione as imagens a serem exportadas.

2. Clique em *Arquivo* → *Exportar* → *Exportar para CD* e clique em *OK*.

   O f-spot copia os arquivos e abre a caixa de diálogo de gravação do CD. Atribua um nome ao disco de imagem e determine a velocidade de gravação. Clique em *Gravar* para iniciar o processo de gravação do CD.

Figura 15.9 *Exportando imagens para o CD*



15.5.6 Processamento básico de imagens com o f-spot

O f-spot oferece diversas funcionalidades básicas de edição de imagens. Para especificar o modo de edição do f-spot, clique no ícone *Editar Imagem* na barra de ferramentas ou clique duas vezes na imagem para editá-la. Alterne imagens usando as teclas de seta na parte inferior direita. Escolha entre as funções de edição a seguir:

Focar
: Acesse essa função por meio de *Editar → Focar*. Ajuste os valores de *Quantidade*, *Raio* e *Limite* de acordo com suas necessidades e clique em *OK*.

Cortar Imagem
: Para cortar a imagem conforme selecionado, escolha um corte de proporção fixa ou a opção *Sem Restrições* no menu suspenso na parte inferior esquerda, selecione a região a cortar e clique no ícone de tesoura próximo ao menu de proporção.

Redução de Olho Vermelho
Em um retrato, selecione a região dos olhos do rosto e clique no ícone de olhos vermelhos.

Ajustar Cor
Exiba o histograma usado na criação da imagem e corrija a exposição e a temperatura da cor se necessário.

DICA: Processamento avançado de imagens

A edição profissional de imagens pode ser feita com o GIMP. Mais informações sobre o GIMP podem ser encontradas em Capítulo 17, *Manipulando gráficos com o GIMP* (p 241).

15.6 Mais informações

Para obter mais informações sobre o uso de câmeras digitais com o Linux, consulte os sites da Web a seguir:

- `http://digikam.sourceforge.net/` - Informações sobre o Digikam
- `http://www.gphoto.org` - Informações sobre o gPhoto2
- `http://www.gphoto.org/proj/libgphoto2/support.php` - Uma lista abrangente de câmeras suportadas
- `http://www.thekompany.com/projects/gphoto/` - Informações sobre o Kamera, um front end KDE para o gPhoto2

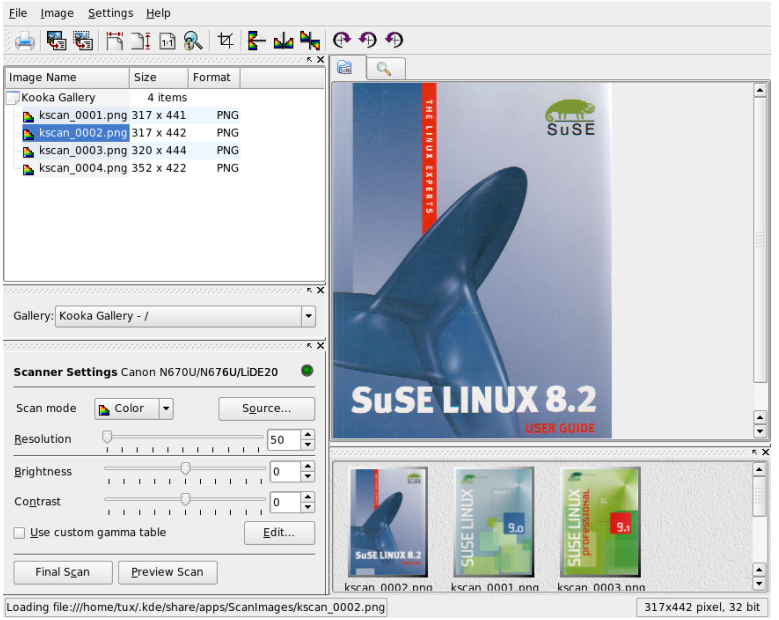
16 Kooka — Aplicativo de digitalização

O Kooka é um aplicativo do KDE para digitalização. Este capítulo explica a interface do usuário e a funcionalidade do aplicativo. Além de criar arquivos de imagens a partir de mídia impressa, como fotografias ou revistas, o Kooka possui recursos de reconhecimento de caracteres. Isso significa que ele pode ser útil na conversão de textos escritos em arquivos de texto editáveis.

Inicie o Kooka a partir do menu principal ou digite o comando `kooka`. Quando iniciado, o Kooka abre uma janela de três frames com uma barra de menus no canto superior esquerdo e, imediatamente abaixo desta, uma barra de ferramentas. Todas as janelas podem ser livremente reajustadas ou reorganizadas com o mouse. Também é possível destacar completamente frames individuais da janela do Kooka e colocá-los em qualquer local da área de trabalho. Para movimentar os frames, clique e arraste a linha dupla fina imediatamente acima do frame. Qualquer frame, exceto a janela principal, pode ser colocado dentro de outro, alinhado à esquerda, à direita, na parte superior ou inferior ou centralizado. As janelas centralizadas têm o mesmo tamanho, são empilhadas e podem ser colocadas em primeiro plano com guias.

Por padrão, os frames *Visualizador de Imagens* e *Visualização da Digitalização* compartilham uma janela. As guias permitem alternar entre eles. O frame esquerdo mostra a galeria. É um pequeno browser de arquivos para acessar as imagens digitalizadas. O frame no canto inferior direito é compartilhado pelo OCR e as miniaturas, que podem ser carregadas no visualizador de imagens com um simples clique do mouse. Consulte a Figura 16.1, “Janela principal do Kooka” (p 234).

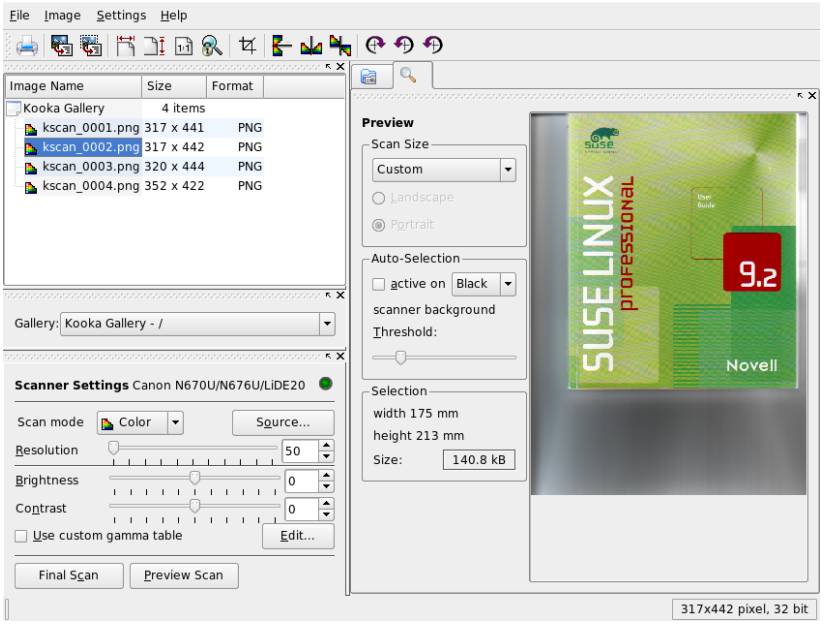
Figura 16.1 *Janela principal do Kooka*



16.1 Visualização

Sempre é adequado criar uma visualização quando o objeto a ser digitalizado é menor que a área de digitalização total. Defina alguns parâmetros à esquerda do frame de visualização. Selecione o tamanho da digitalização com *Personalizado* ou usando os formatos padrão. Consulte a Figura 16.2, “Janela de visualização do Kooka” (p 235). A configuração *Personalizado* é a mais flexível porque permite selecionar a área desejada com o mouse. Depois de definir as configurações, visualize a imagem a ser digitalizada clicando em *Pré-visualização da Digitalização* em *Parâmetros da Digitalização*.

Figura 16.2 *Janela de visualização do Kooka*

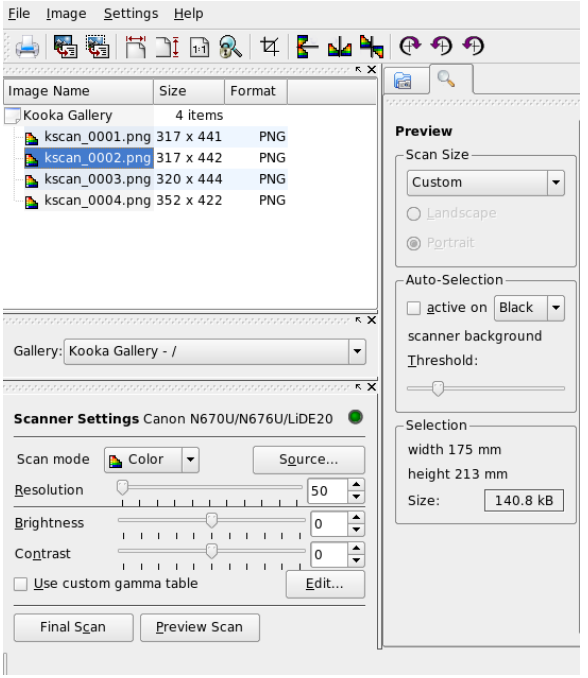


16.2 Digitalização final

Se você selecionou *Personalizado* para o tamanho da digitalização, use o mouse para selecionar a área retangular a ser digitalizada. A área selecionada é delimitada por uma borda pontilhada.

Escolha entre digitalização em preto e branco e em cores e defina a resolução com o controle deslizante. Consulte a Figura 16.3, “Parâmetros de digitalização do Kooka” (p 236). Quanto maior for a resolução, melhor será a qualidade da imagem digitalizada. No entanto, isso também resulta em um arquivo igualmente maior, e o processo de digitalização poderá ser mais demorado com resoluções mais altas. Ative *Usar tabela de gamas personalizados* e clique em *Editar* para alterar as configurações de brilho, contraste e gama.

Figura 16.3 *Parâmetros de digitalização do Kooka*



Depois de definir todas as configurações, clique em *Digitalização Final* para digitalizar a imagem. A imagem digitalizada é exibida como uma miniatura no visualizador de imagens. Quando solicitado, selecione o formato para gravação da imagem. Para gravar todas as imagens futuras nesse mesmo formato, marque a caixa correspondente. Confirme com *OK*.

16.3 Menus

Algumas funções da barra de ferramentas também estão disponíveis nos menus *Arquivo* e *Imagem*. Modifique as configurações de preferências do Kooka em *Configurações*.

Arquivo

Use este menu para iniciar o assistente de impressão KPrinter, criar uma nova pasta para suas imagens e gravar, apagar e fechar arquivos. Os resultados OCR de um

documento de texto digitalizado podem ser gravados aqui. Use esse menu também para fechar o Kooka.

Image (Imagem)
O menu *Imagem* permite iniciar um aplicativo gráfico de pós-processamento ou reconhecimento ótico de caracteres de uma imagem. O texto reconhecido de uma operação OCR é exibido em seu próprio frame. Estão disponíveis várias ferramentas para dimensionar, girar e inverter as imagens. Essas funções também podem ser acessadas na barra de ferramentas. O submenu *Criar da Seleção* permite gravar uma área de uma imagem anteriormente marcada com o mouse.

Configurações

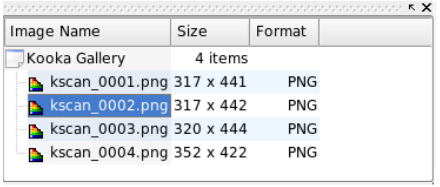
Configurações ajusta a aparência e o funcionamento do Kooka. É possível ativar e desativar a barra de ferramentas e a barra de status e definir atalhos de teclados para entradas do menu. *Configurar Barra de Ferramentas* oferece uma lista de todas as funções disponíveis para a barra de ferramentas. *Configurar Kooka* abre uma caixa de diálogo de configuração para modificar a aparência e funcionamento do Kooka. Normalmente, no entanto, os padrões são suficientes. Nas *Visualizações de Ferramentas*, ative e desative o visualizador de miniaturas, a visualização, a galeria, os parâmetros de digitalização e a janela de resultados OCR.

Ajuda
O menu *Ajuda* oferece acesso ao manual de ajuda online do Kooka. Use-o também para acessar um canal de informações sobre problemas e sugestões. Ele também fornece informações sobre a versão, os autores e a licença do Kooka e do KDE.

16.4 Galeria

A janela da galeria mostra a pasta padrão na qual o Kooka armazena todos os seus arquivos de imagens. A Figura 16.4, “Galeria do Kooka” (p 238) mostra um exemplo. Para gravar uma imagem em seu diretório pessoal principal, clique na miniatura e selecione *Arquivo → Gravar Imagem*. Em seguida, digite seu diretório pessoal principal e dê ao arquivo um nome descritivo.

Figura 16.4 *Galeria do Kooka*

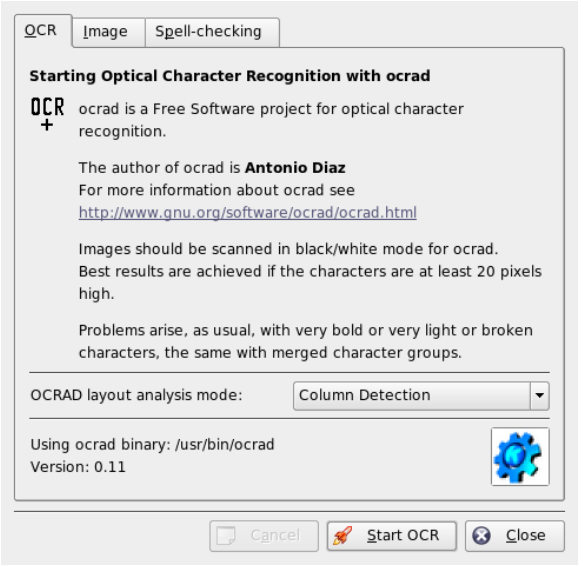


Para adicionar imagens à galeria, arraste-as do Konqueror e solte-as. Inicie o Konqueror, navegue até o diretório que contém as imagens a serem adicionadas à galeria e arraste-as com o mouse, soltando-as em uma pasta da galeria do Kooka.

16.5 Reconhecimento Óptico de Caracteres

Se o módulo de reconhecimento de caracteres estiver instalado, os documentos poderão ser digitalizados no modo *vetorial*, gravados no formato proposto e processados para reconhecimento de texto no menu *Imagem*. Processe o documento inteiro ou apenas uma área previamente selecionada. A caixa de diálogo informa ao módulo se o texto original é do tipo impresso, manuscrito ou padronizado. Defina também o idioma para que o módulo possa processar o documento corretamente. Consulte a Figura 16.5, “OCR com o Kooka” (p 239).

Figura 16.5 *OCR com o Kooka*


OCR
Image
Spell-checking
Starting Optical Character Recognition with ocrad
OCR
ocrad is a Free Software project for optical character recognition.
The author of ocrad is Antonio Diaz
For more information about ocrad see
http://www.gnu.org/software/ocrad/ocrad.html
Images should be scanned in black/white mode for ocrad.
Best results are achieved if the characters are at least 20 pixels high.
Problems arise, as usual, with very bold or very light or broken characters, the same with merged character groups.
OCRAD layout analysis mode:
Column Detection
Using ocrad binary: /usr/bin/ocrad
Version: 0.11
Cancel
Start OCR
Close

Alterne para a janela *Texto Resultado do OCR* e verifique se o texto precisa ser revisado. Para isso, grave-o com *Arquivo → Salvar Texto Resultado do OCR*. O texto poderá ser processado com o OpenOffice.org ou com o KWrite.

17 Manipulando gráficos com o GIMP

O GIMP (*GNU Image Manipulation Program*) é um programa de criação e edição de gráficos de pixels. Em quase todos os aspectos, seus recursos são comparáveis aos recursos do Adobe Photoshop e de outros programas comerciais. Use-o para redimensionar e retocar fotografias, desenhar imagens para páginas da Web, criar capas para CDs personalizados ou praticamente qualquer outro projeto gráfico. Ele atende às necessidades de amadores e profissionais.

Como vários outros programas do Linux, o GIMP é desenvolvido com o esforço conjunto de desenvolvedores do mundo inteiro que oferecem voluntariamente seu tempo e código para o projeto. O programa está em constante desenvolvimento. Por isso, a versão incluída no seu SUSE Linux poderá variar ligeiramente da versão mencionada aqui. O layout das janelas e seções individuais é o item que mais pode variar.

O GIMP é um programa extremamente complexo. Apenas alguns recursos, ferramentas e itens de menu serão discutidos neste capítulo. Consulte a Seção 17.6, “Para obter mais informações” (p 248) para saber onde encontrar mais informações sobre o programa.

17.1 Formatos gráficos

Existem dois formatos principais de gráficos: pixel e vetor. O GIMP funciona apenas com gráficos de pixels, que é o formato normal de fotografias e imagens digitalizadas. Os gráficos de pixels consistem em pequenos blocos de cores que, reunidos, criam uma imagem completa. Os arquivos podem facilmente aumentar por causa disso. Não é possível aumentar o tamanho da imagem de pixel sem perder qualidade.

Ao contrário dos gráficos de pixels, os gráficos de vetor não armazenam informações para cada pixel individual. Em vez disso, eles armazenam informações sobre como os pontos, linhas ou áreas da imagem são agrupados. As imagens de vetor também podem ser facilmente dimensionadas. O aplicativo de desenho do OpenOffice.org, por exemplo, usa esse formato.

17.2 Iniciando o GIMP

Inicie o GIMP no menu principal. Outra opção é digitar `gimp &` na linha de comando.

17.2.1 Configuração inicial

Quando o GIMP é iniciado pela primeira vez, um assistente de configuração é aberto para a configuração preparatória. As configurações padrão são aceitáveis para a maioria das finalidades. Pressione *Continuar* em cada caixa de diálogo, a menos que você esteja familiarizado com as configurações e prefira escolher outras.

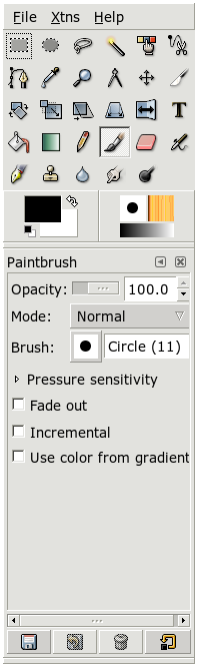
17.2.2 Janelas padrão

Por padrão, três janelas são exibidas. Elas podem ser organizadas na tela e, com exceção da caixa de ferramentas, podem ser fechadas quando não forem mais necessárias. Ao fechar a caixa de ferramentas, você fecha o aplicativo. Na configuração padrão, o GIMP grava o layout de janela quando você sai do programa. As caixas de diálogo deixadas abertas reaparecem quando você reinicia o programa.

Caixa de ferramentas

A janela principal do GIMP, como mostra a Figura 17.1, “Janela principal” (p 243), contém os controles principais do aplicativo. Ao fechar a janela, você sai do aplicativo. Na parte superior, a barra de menus oferece acesso a funções de arquivos, extensões e ajuda. Abaixo dela, estão os ícones de várias ferramentas. Passe o mouse sobre o ícone para exibir informações sobre a ferramenta.

Figura 17.1 *Janela principal*



As cores de primeiro e segundo plano são mostradas em duas caixas sobrepostas. As cores padrão são preto para segundo plano e branco para primeiro plano. Clique na caixa para abrir uma caixa de diálogo de seleção de cor. Troque as cores de primeiro e segundo plano usando o símbolo de seta dobrada localizado no canto superior direito das caixas. Use o símbolo em preto e branco no canto inferior esquerdo para redefinir as cores com a configuração padrão.

À direita, são mostrados o pincel, o padrão e o gradiente atuais. Clique no que estiver exibido para acessar a caixa de diálogo de seleção. A parte inferior da janela permite configurar várias opções para a ferramenta atual.

Camadas, canais, caminhos, desfazer

Na primeira seção, use a caixa suspensa para selecionar a imagem à qual a guia se refere. Clicando em *Automático*, controle se a imagem ativa será escolhida automaticamente. Por padrão, *Automático* estará habilitado.

A opção *Camadas* mostra os diferentes níveis nas imagens atuais e pode ser usada para manipular as camadas. *Canais* mostra e pode manipular os canais de cores da imagem.

Os caminhos são um método avançado de selecionar partes de uma imagem. Eles também podem ser usados para desenhar. *Caminhos* mostra os caminhos disponíveis para uma imagem e oferece acesso às suas funções. *Desfazer* mostra um histórico limitado de modificações feitas na imagem atual.

A parte inferior da janela contém três guias. Com elas, selecione o pincel, o gradiente e o padrão atuais.

17.3 Noções básicas do GIMP

Embora o GIMP possa ser um tanto complexo para usuários novos, a maioria logo descobre que ele é fácil de usar depois de conhecer algumas funções básicas. As funções básicas cruciais são criação, abertura e gravação de imagens.

17.3.1 Criando uma nova imagem

Para criar uma nova imagem, selecione *Arquivo* → *Novo* ou pressione Ctrl + N. Será aberta uma caixa de diálogo onde você poderá configurar a nova imagem. Se desejar, use *Modelo* para selecionar um modelo no qual sua nova imagem se baseará. O GIMP inclui vários modelos, desde folha de papel A4 até capa de CD. Para criar um modelo personalizado, selecione *Arquivo* → *Diálogos* → *Modelos* e use os controles oferecidos pela janela aberta.

Na seção *Tamanho da Imagem*, defina o tamanho da imagem a ser criada em pixels ou em outra unidade. Clique na unidade para selecionar outra na lista de unidades disponíveis. A proporção entre pixels e unidade é definida em *Resolução*, que é exibida quando a seção *Opções Avançadas* é aberta. Uma resolução de 72 pixels por polegada corresponde à exibição de tela. Ela é suficiente para imagens de páginas da Web. Use uma resolução mais alta para as imagens a serem impressas. Na maioria das impressoras, a resolução de 300 pixels por polegada produz qualidade aceitável.

Em *Espaço de cor*, escolha se a imagem deve estar em cores (*RGB*) ou *Tons de cinza*. Selecione o *Tipo de Preenchimento* para a nova imagem. *Cor de Frente* e *Cor de Fundo* usam as cores selecionadas na caixa de ferramentas. *Branco* usa um segundo plano branco na imagem. *Transparente* cria uma imagem transparente. A *transparência* é

representada por um padrão quadriculado cinza. Digite um comentário para a nova imagem em *Comentário*.

Quando estiver satisfeito com as configurações, clique em *OK*. Para restaurar as configurações padrão, pressione *Reiniciar*. Pressionando *Cancelar*, você cancela a criação de uma nova imagem.

17.3.2 Abrindo uma imagem existente

Para abrir uma imagem existente, selecione *Arquivo* → *Abrir* ou pressione Ctrl + O. Na caixa de diálogo exibida, selecione o arquivo desejado. Clique em *OK* para abrir a imagem selecionada. Pressione *Cancelar* para não abrir a imagem.

17.3.3 Janela da imagem

A nova imagem ou a imagem aberta aparece em sua própria janela. A barra de menus na parte superior da janela oferece acesso a todas as funções de imagem. Você também pode acessar o menu clicando o botão direito na imagem ou clicando no pequeno botão de seta no canto esquerdo das réguas.

Arquivo oferece as opções padrão de arquivo, como *Salvar* e *Imprimir*. *Fechar* fecha a imagem exibida. *Encerrar* fecha todo o aplicativo.

Com os itens do menu *Exibir*, controle a exibição da imagem e da sua janela. *Nova Visão* abre uma segunda janela com a imagem atual. As alterações feitas em uma tela são refletidas em todas as outras telas da mesma imagem. Telas alternadas são úteis para aumentar uma parte da imagem que está sendo manipulada e, ao mesmo tempo, ver a imagem completa em outra tela. Ajuste o nível de aumento da janela atual usando *Zoom*. Quando *Ajustar Janela à Imagem* é selecionada, a janela da imagem é redimensionada para caber exatamente na exibição da imagem atual.

17.4 Gravando imagens

Nenhuma função de imagem é tão importante como *Arquivo* → *Salvar*. É melhor gravar várias vezes que raramente. Use *Arquivo* → *Salvar como* para gravar a imagem com um novo nome de arquivo. É uma boa idéia gravar fases da imagem com nomes

diferentes ou fazer backups em outro diretório. Assim, você pode restaurar facilmente um estado anterior.

Ao gravar pela primeira vez ou usar *Salvar como*, é exibida uma caixa de diálogo para que você especifique o nome e o tipo do arquivo. Digite o nome do arquivo no campo na parte superior. Para *Salvar na pasta*, selecione o diretório no qual deseja salvar o arquivo de uma lista de diretórios usados normalmente. Para usar um diretório diferente ou criar um novo, abra a opção *Navegar para outras pastas*. Recomendamos deixar *Selecionar Tipo de Arquivo* definido como *Por Extensão*. Com essa configuração, o GIMP determina o tipo de arquivo com base na extensão anexada ao seu nome. Os seguintes tipos de arquivos são freqüentemente úteis:

XCF
: Esse é o formato nativo do aplicativo. Ele grava todas as informações de camada e caminho junto com a própria imagem. Mesmo que você precise de uma imagem em outro formato, geralmente é uma boa idéia gravar uma cópia como XCF para simplificar futuras modificações.

PAT
: Esse é o formato usado por padrões GIMP. Gravar uma imagem nesse formato permite usá-la como padrão de preenchimento no GIMP.

JPG
: JPG ou JPEG é um formato comum para fotografias e imagens de páginas da Web sem transparência. Seu método de compactação permite reduzir o tamanho do arquivo, mas algumas informações são perdidas na compactação. Pode ser uma boa idéia usar a opção de visualização ao ajustar o nível de compactação. Os níveis de 85% a 75% freqüentemente resultam em qualidade de imagem aceitável com compactação razoável. Também é recomendado gravar um backup em formato sem perdas, como o XCF. Se estiver editando uma imagem, grave apenas a imagem finalizada no formato JPG. O carregamento repetido de JPG e a sua gravação resultam rapidamente em baixa qualidade de imagem.

GIF
: Embora muito popular no passado para gráficos com transparência, o GIF é menos usado agora por motivos de licença. O GIF também é usado para imagens animadas. O formato só grava imagens *indexadas*. Geralmente, o tamanho do arquivo pode ser pequeno se apenas algumas cores são usadas.

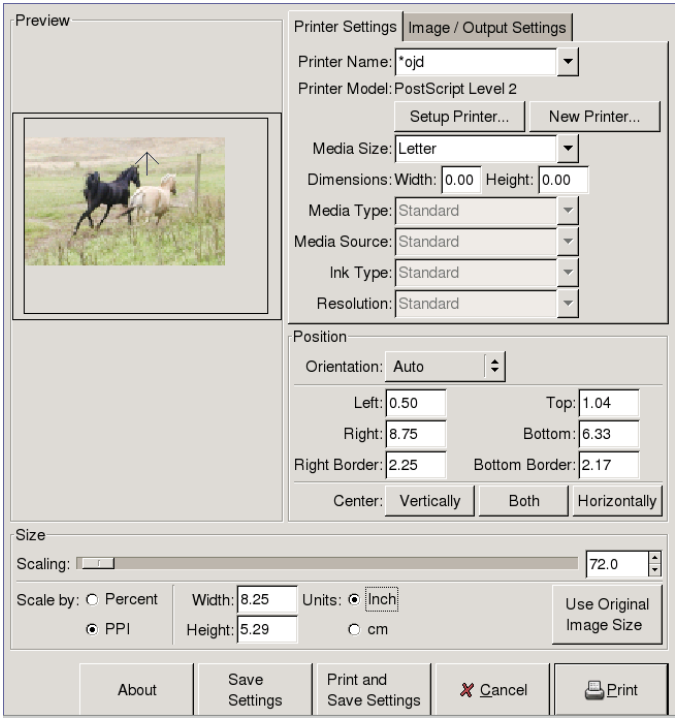
PNG
: Com suporte a transparências, compactação sem perdas, disponibilidade gratuita e crescente suporte a browsers, o PNG vem substituindo o GIF como o formato preferido de imagens da Web com transparência. Uma vantagem adicional: o PNG oferece transparência parcial, o que não ocorre com o GIF. Isso permite transições mais suaves de áreas coloridas para áreas transparentes (*suavização*).

Para gravar a imagem no formato escolhido, pressione *Salvar*. Para interromper, pressione *Cancelar*. Se a imagem possuir recursos que não podem ser gravados no formato escolhido, será exibida uma caixa de diálogo com opções para solucionar o problema. Escolher *Exportar*, se oferecido, normalmente produz os resultados esperados. Uma janela é aberta exibindo as opções de formato. São fornecidos valores padrão razoáveis.

17.5 Imprimindo imagens

Para imprimir uma imagem, selecione *Arquivo* → *Imprimir* no menu da imagem. Se a sua impressora estiver configurada no SUSE, ela deverá aparecer na lista. Em alguns casos, pode ser necessário selecionar um driver adequado em *Configurar Impressora*. Selecione o tamanho de papel apropriado em *Tamanho da Mídia* e o tipo em *Tipo de Mídia*. Outras configurações estão disponíveis na guia *Imagem/Configurações de Saída*.

Figura 17.2 *Caixa de diálogo de impressão*



Na parte inferior da janela, ajuste o tamanho da imagem. Pressione *Usar Tamanho Original da Imagem* para usar as configurações da própria imagem. Isso é recomendado se você define um tamanho de impressão e uma resolução adequados na imagem. Ajuste a posição da imagem na página com os campos de *Posição* ou arrastando a imagem em *Pré-visualização*.

Quando estiver satisfeito com as configurações, pressione *Imprimir*. Para gravar as configurações para uso futuro, use *Imprimir e Salvar Configurações*. *Cancelar* interrompe a impressão.

17.6 Para obter mais informações

Veja abaixo alguns recursos úteis para o usuário do GIMP. Infelizmente, muitos recursos se aplicam a versões mais antigas.

- A *Ajuda* oferece acesso ao sistema de ajuda interno. Esta documentação também está disponível nos formatos HTML e PDF em `http://docs.gimp.org`.

- O Grupo de Usuários do GIMP disponibiliza um site informativo e interessante em `http://gug.sunsite.dk`.

- A home page oficial do GIMP é `http://www.gimp.org`.

- *Grokking the GIMP*, escrito por Carey Bunks, é um excelente livro sobre uma versão mais antiga do GIMP. Embora alguns aspectos do programa tenham mudado, a obra pode oferecer ótimas orientações sobre manipulação de imagens. Uma versão online está disponível em `http://gimp-savvy.com/BOOK/`.

- `http://gimp-print.sourceforge.net` é a página da Web do plug-in de impressão do GIMP. O manual do usuário disponível no site fornece informações detalhadas sobre a configuração e o uso do programa.

Parte VI Mobilidade

18 Computação móvel com o Linux

Este capítulo oferece uma visão geral dos diversos aspectos relativos ao uso do Linux para computação móvel. Há uma breve introdução dos diversos campos de uso e uma descrição dos recursos essenciais do hardware empregado. As soluções de software para requisitos e opções especiais de máximo desempenho são abordadas juntamente com possibilidades para minimizar o consumo de energia. O capítulo termina com uma visão geral das fontes de informação mais importantes sobre o assunto.

A maioria das pessoas associa a computação móvel a laptops, PDAs e telefones celulares, e ao intercâmbio de dados entre esses aparelhos. Este capítulo amplia o foco para componentes de hardware móveis, como discos rígidos externos, unidades flash ou câmeras digitais, que podem ser conectados a laptops ou sistemas de desktop.

18.1 Laptops

O hardware de laptops difere do hardware de um sistema de desktop normal. Isso ocorre porque critérios como intercambiamento, espaço ocupado e consumo de energia são propriedades relevantes. Os fabricantes de hardware móvel desenvolveram o padrão PCMCIA (Personal Computer Memory Card International Association - Associação Internacional de Cartões de Memória para Computadores Pessoais). Esse padrão abrange cartões de memória, placas de interface de rede, ISDN e placas de modem, além de discos rígidos externos. A forma como o suporte para tal hardware é implementado no Linux, os pontos a serem levados em consideração durante a configuração, qual software está disponível para o controle do PCMCIA e como solucionar quaisquer possíveis problemas são descritos em Capítulo 19, *PCMCIA* (p 263).

18.1.1 Conservação de energia

A inclusão de componentes de sistema com otimização de energia durante a fabricação de laptops contribui para a sua adequação ao uso sem acesso à rede elétrica. A contribuição desses componentes para a preservação de energia é, ao menos, tão importante quanto a do sistema operacional. O SUSE Linux dá suporte a diversos métodos que influenciam o consumo de energia de um laptop e surtem efeitos variáveis sobre o tempo de operação com a carga da bateria. A lista a seguir está em ordem decrescente de contribuição para a conservação de energia:

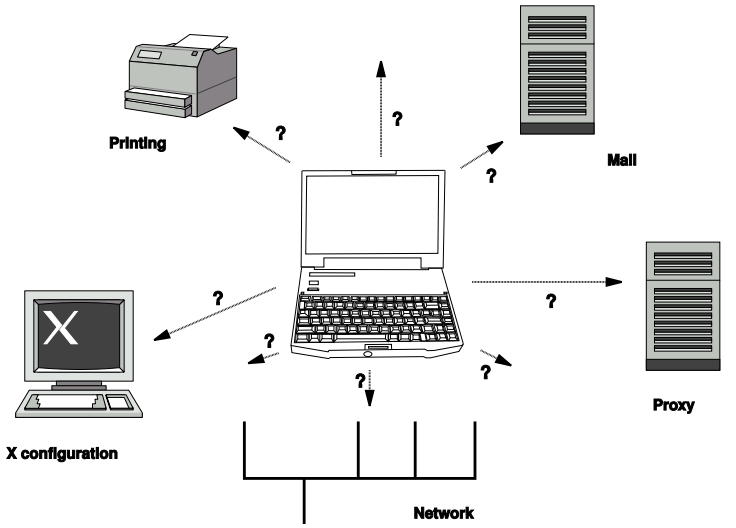
- Regulagem da velocidade da CPU
- Desativação da iluminação da tela durante pausas
- Ajuste manual da iluminação da tela
- Desconexão de acessórios não utilizados e habilitados para hotplug (CD-ROM USB, mouse externo, placas PCMCIA não utilizadas etc.)
- Colocar o disco rígido em modo de espera quando inativo

Informações de apoio detalhadas sobre o gerenciamento de energia no SUSE Linux e sobre a operação do módulo de gerenciamento de energia YaST podem ser encontradas em Capítulo 21, *Gerenciamento de energia* (p 277).

18.1.2 Integração em ambientes operacionais variáveis

Seu sistema precisa se adaptar a ambientes operacionais variáveis quando for usado para a computação móvel. Vários serviços dependem do ambiente e os clientes subjacentes precisam ser reconfigurados. O SUSE Linux se encarrega dessa tarefa para você.

Figura 18.1 *Integrando um laptop em uma rede*



Os serviços afetados no caso de um laptop que transita entre uma pequena rede doméstica e uma rede de escritório são:

Configuração de rede
: Inclui a atribuição de endereço IP, a resolução do nome, a conectividade à Internet e a conectividade a outras redes.

Impressão
: Precisam estar presentes um banco de dados atual de impressoras disponíveis e um servidor de impressão disponível, dependendo da rede.

E-Mail e proxies
: Assim como ocorre com a impressão, a lista dos servidores correspondentes precisa ser atual.

Configurando X
: Se o seu laptop estiver temporariamente conectado a um projetor ou monitor externo, as diferentes configurações de exibição precisam estar disponíveis.

O SUSE Linux oferece duas opções de integração de um laptop a ambientes operacionais existentes. Essas opções podem ser combinadas.

SCPM
O SCPM (system configuration profile management - gerenciamento de perfil de configuração do sistema) permite o armazenamento de estados de configuração arbitrários de um sistema em um tipo de “instantâneo” chamado de *perfil*. Os perfis podem ser criados para diferentes situações. Eles são úteis quando um sistema é operado em ambientes variáveis (rede doméstica, rede de escritório). Sempre é possível alternar entre perfis. Informações sobre o SCPM podem ser encontradas em Capítulo 20, *System Configuration Profile Management* (p 265). O applet Seletor de Perfil do kicker no KDE permite alternar entre perfis. O aplicativo requer a senha do root antes de alternar.

SLP
O SLP (Service Location Protocol) simplifica a conexão de um laptop a uma rede existente. Sem o SLP, o administrador do laptop normalmente necessita ter conhecimentos detalhados sobre os serviços disponíveis em uma rede. O SLP transmite a disponibilidade de um determinado tipo de serviço a todos os clientes de uma rede local. Os aplicativos que dão suporte ao SLP podem processar as informações despachadas pelo SLP e podem ser configurados automaticamente. O SLP pode até ser usado para instalar um sistema e poupar o esforço de busca de uma fonte de instalação adequada. Informações detalhadas sobre o SLP podem ser encontradas em Capítulo 39, *Serviços SLP na rede* (p 629).

O ponto forte do SCPM é a habilitação e a manutenção de condições de sistema reproduzíveis. O SLP torna a configuração de um computador em rede bem mais fácil, automatizando boa parte desse processo.

18.1.3 Opções de software

Diversas áreas de tarefas especiais no uso móvel são abrangidas por software dedicado: monitoramento do sistema (principalmente a carga da bateria), sincronização de dados e comunicação sem fio com periféricos e a Internet. As seções a seguir tratam dos aplicativos mais importantes oferecidos pelo SUSE Linux para cada tarefa.

Monitoramento do sistema

Duas ferramentas de monitoramento do sistema KDE são oferecidas pelo SUSE Linux. O applet KPowersave no kicker exibe o status simples da bateria recarregável do laptop. O monitoramento de sistema complexo é realizado pelo KSysguard. Quando você usa

o GNOME, as funções descritas são fornecidas pelo ACPI (como um applet do painel) do GNOME e pelo Monitor do Sistema.

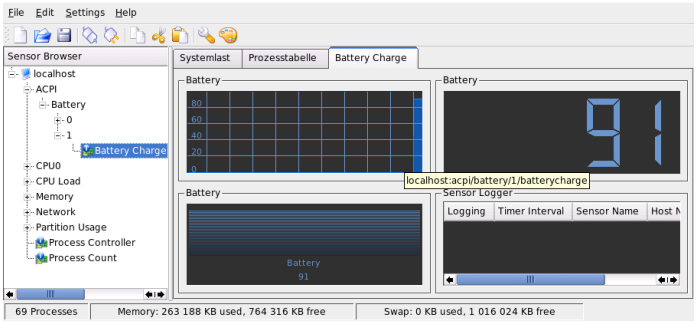
KPowersave

O KPowersave é um applet que exibe o estado da bateria recarregável no painel de controle. O ícone se ajusta de modo a representar o tipo de fonte de energia. Ao trabalhar em corrente alternada, um pequeno ícone de plug é exibido. Ao trabalhar com bateria, o ícone se transforma em uma bateria. O menu correspondente abre o módulo YaST de gerenciamento de energia após solicitar a senha do root. Desse modo, é possível configurar o comportamento do sistema com diferentes tipos de fontes de energia. Informações sobre o gerenciamento de energia e sobre o módulo YaST correspondente podem ser encontradas em Capítulo 21, *Gerenciamento de energia* (p 277).

KSysguard

O KSysguard é um aplicativo independente que reúne todos os parâmetros mensuráveis do sistema em um único ambiente de monitoramento. O KSysguard possui monitores de ACPI (status da bateria), carga da CPU, rede, particionamento e uso da memória. Ele também pode observar e exibir todos os processos do sistema. A apresentação e filtragem dos dados coletados podem ser personalizadas. É possível monitorar diferentes parâmetros do sistema em diversas páginas de dados ou coletar os dados de diversas máquinas em paralelo na rede. O KSysguard também pode ser executado como um daemon em máquinas desprovidas de um ambiente KDE. Mais informações sobre esse programa são fornecidas na sua função de ajuda integrada ou nas páginas de ajuda do SUSE.

Figura 18.2 *Monitorando o status da bateria com o KSysguard*



Sincronizando dados

Ao alternar entre o trabalho em uma máquina móvel desconectada da rede e o trabalho em uma estação em rede em um escritório, é necessário manter a sincronização dos dados processados em todas as instâncias. Isso pode incluir pastas de e-mail, diretórios e arquivos individuais que precisam estar presentes tanto para o trabalho remoto como para o trabalho no escritório. A solução nos dois casos é a seguinte:

Sincronização de e-mail
: Use uma conta IMAP para armazenar seus e-mails na rede do escritório. Os e-mails passam a ser acessados da estação de trabalho com o uso de qualquer cliente de e-mail desconectado habilitado para IMAP, como o Mozilla Thunderbird Mail, o Evolution ou o KMail, conforme descrito na *Inicialização*. O cliente de e-mail precisa ser configurado de tal modo que as `Mensagens enviadas` sejam sempre acessadas da mesma pasta. Isso assegura a disponibilidade de todas as mensagens com informações sobre seu status após a conclusão do processo de sincronização. Use um servidor SMTP implementado no cliente de e-mail para o envio de mensagens, em vez do postfix ou do sendmail do MTA em todo o sistema, para receber retorno confiável sobre e-mails não enviados.

Sincronizando arquivos e diretórios
: Existem diversos utilitários adequados para a sincronização de dados entre um laptop e uma estação de trabalho. Para obter informações detalhadas, consulte Capítulo 47, *Sincronização de arquivos* (p 759).

Comunicação sem fio

Além da conexão a redes domésticas ou de escritórios com um cabo, também é possível fazer uma conexão sem fio de um laptop a outros computadores, periféricos, telefones celulares ou PDAs. O Linux dá suporte a três tipos de comunicação sem fio:

WLAN
: Com o maior alcance dessas tecnologias sem fio, o WLAN é a única adequada para a operação de redes de grande porte e, às vezes, até mesmo de redes desconectadas virtualmente. Máquinas individuais podem se conectar entre si para formar uma rede sem fio independente ou para acessar a Internet. Dispositivos chamados de pontos de acesso atuam como estações de base para dispositivos habilitados para WLAN, além de servir como intermediários para o acesso à Internet. Um usuário móvel pode alternar entre pontos de acesso dependendo do local e de que ponto de

acesso ofereça a melhor conexão. Assim como na telefonia celular, uma rede de grande porte está disponível aos usuários da WLAN sem restringi-los a um local específico para o acesso. Detalhes sobre a WLAN podem ser encontrados em Seção 22.1, “LAN sem fio” (p 303).

Bluetooth
O Bluetooth possui o mais amplo espectro de aplicação de todas as tecnologias sem fio. Ele pode ser usado na comunicação entre computadores (laptops) e PDAs ou telefones celulares, assim como o IrDA. Também pode ser utilizado para conectar diversos computadores dentro de uma faixa visível. O Bluetooth também é usado para conectar componentes sem fio do sistema, como um teclado ou mouse. Entretanto, o alcance dessa tecnologia não é suficiente para conectar sistemas remotos a uma rede. A WLAN é a melhor opção de tecnologia para comunicações em locais com obstáculos físicos, como paredes. Mais informações sobre o Bluetooth, suas aplicações e sua configuração podem ser encontradas em Seção 22.2, “Bluetooth” (p 314).

IrDA
O IrDA é a tecnologia sem fio de menor alcance. As duas extremidades da comunicação precisam estar a uma distância visível uma da outra. Não é possível contornar obstáculos como paredes. Uma aplicação possível do IrDA é a transmissão de arquivos de um laptop para um telefone celular. O curto caminho do laptop para o telefone celular é coberto com o uso do IrDA. O transporte de longo alcance do arquivo ao seu destinatário é feito pela rede móvel. Outra aplicação do IrDA é a transmissão sem fio de serviços de impressão no escritório. Mais informações sobre o IrDA podem ser encontradas em Seção 22.3, “Transmissão de dados infravermelhos” (p 325).

18.1.4 Segurança de dados

Em termos ideais, os dados contidos no seu laptop são protegidos de diversas maneiras contra o acesso não autorizado. Possíveis medidas de segurança podem ser tomadas nas seguintes áreas:

Proteção contra roubo
Sempre que possível proteja a integridade física do seu sistema contra roubo. Diversas ferramentas de segurança, como correntes, podem ser adquiridas em lojas varejistas.

Protegendo dados no sistema

Dados importantes devem ser criptografados não apenas durante a transmissão, mas também no disco rígido. Essa medida assegura sua segurança em caso de roubo. A criação de uma partição criptografada com o SUSE Linux é descrita em Seção 23.3, “Criptografando partições e arquivos” (p 348).

IMPORTANTE: Segurança de dados e o evento Suspender para Disco

As partições criptografadas não são desmontadas durante um evento de suspender para disco. Assim, todos os dados contidos nessas partições ficarão disponíveis para qualquer pessoa que conseguir roubar o hardware e inicializar o disco rígido.

Segurança de rede

Qualquer transferência de dados deve ser protegida, independentemente de como seja feita. Questões gerais de segurança relativas ao Linux e a redes podem ser encontradas em Seção 23.4, “Segurança e confidencialidade” (p 351). Medidas de segurança referentes a redes sem fio são fornecidas em Capítulo 22, *Comunicação sem fio* (p 303).

18.2 Hardware móvel

O SUSE Linux dá suporte à detecção automática de dispositivos de armazenamento móveis no Firewire (IEEE 1394) ou USB. O termo *dispositivo de armazenamento móvel* se aplica a qualquer tipo de disco rígido Firewire ou USB, unidade flash USB ou câmera digital. Esses dispositivos são automaticamente detectados e configurados por meio do sistema hotplug logo que são conectados ao sistema pela interface correspondente. O subfs e o submount asseguram a montagem dos dispositivos nos locais correspondentes no sistema de arquivos. O usuário é totalmente poupado da montagem e desmontagem manuais encontradas em versões anteriores do SUSE Linux. Um dispositivo pode ser simplesmente desconectado quando não houver nenhum programa acessando-o.

Discos rígidos externos (USB e Firewire)

Logo após o correto reconhecimento de um disco rígido externo pelo sistema, seu ícone aparece em *Meu Computador* (KDE) ou em *Computador* (GNOME), na lista de unidades montadas. Clique no ícone para exibir o conteúdo da unidade. É possível criar pastas e arquivos aqui, além de editá-los ou apagá-los. Para mudar o nome que um disco rígido recebeu do sistema, clique o botão direito do mouse no ícone e

selecione o item correspondente no menu. Essa mudança de nome é limitada à exibição no gerenciador de arquivos. O descritor pelo qual o dispositivo é montado em `/media/usb-xxx` ou `/media/ieee1394-xxx` não é afetado.

Unidades flash USB
Esses dispositivos são tratados pelo sistema como discos rígidos externos. Também nesses dispositivos é possível renomear as entradas do gerenciador de arquivos.

Câmeras digitais (USB e Firewire)
As câmeras digitais reconhecidas pelo sistema também aparecem como unidades externas na visão geral do gerenciador de arquivos. O KDE permite a leitura e o acesso às imagens no URL `camera:/`. Essas imagens podem ser processadas com o Digikam ou o GIMP. Ao usar o GNOME, o Nautilus exibe as imagens em sua própria pasta. Um utilitário simples de processamento e gerenciamento de imagens é o f-spot. O processamento avançado de fotos é feito com o GIMP. Para obter mais detalhes sobre câmeras digitais e sobre o gerenciamento de imagens, consulte Capítulo 15, *Câmeras digitais e Linux* (p 211).

18.3 Telefones celulares e PDAs

Tanto um sistema de desktop como um laptop podem se comunicar com um telefone celular via Bluetooth ou IrDA. Alguns modelos dão suporte aos dois protocolos; outros, somente a um dos dois. As áreas de uso dos dois protocolos e a documentação ampliada correspondente já foram citadas em “Comunicação sem fio” (p 258). A configuração desses protocolos nos telefones celulares é descrita nos respectivos manuais. A configuração do componente Linux é descrita em Seção 22.2, “Bluetooth” (p 314) e Seção 22.3, “Transmissão de dados infravermelhos” (p 325).

O suporte à sincronização com dispositivos portáteis fabricados pela Palm, Inc., já vem incorporado ao Evolution e ao Kontact. Nos dois casos, a conexão inicial com o dispositivo é facilmente realizada com um assistente. Após a configuração do suporte para Palm Pilots, é necessário determinar que tipo de dados deve ser sincronizado (endereços, compromissos etc.). Os dois aplicativos de groupware são descritos na *Inicialização*.

O programa KPilot, conforme integração no Kontact, também está disponível como um utilitário independente. Sua descrição está na *Inicialização*. O programa KitchenSync também está disponível para a sincronização de dados de endereços.

18.4 Mais informações

O ponto central de referência para todas as dúvidas relativas a dispositivos móveis e o Linux é http://tuxmobil.org/. Diversas seções desse site da Web tratam de aspectos de hardware e software de laptops, PDAs, telefones celulares e outros hardwares móveis.

Uma abordagem semelhante de http://tuxmobil.org/ é feita por http://www.linux-on-laptops.com/. Informações sobre laptops e dispositivos portáteis podem ser encontradas nesse local.

O SUSE mantém uma lista de discussão em alemão dedicada a laptops. Consulte http://lists.suse.com/archive/suse-laptop/. Nessa lista, usuários e desenvolvedores discutem todos os aspectos da computação móvel com o uso do SUSE Linux. As mensagens em inglês são respondidas, mas a maioria das informações dos arquivos está disponível somente em alemão.

No caso de problemas com o gerenciamento de energia com o SUSE Linux em laptops, é recomendável ler o arquivo README em /usr/share/doc/packages/powersave. Como muitas vezes contém comentários bem recentes de testadores e desenvolvedores, esse diretório oferece dicas valiosas para a solução de problemas.

19 PCMCIA

Esta seção discute aspectos especiais do hardware e do software PCMCIA encontrados em laptops. PCMCIA é o acrônimo de *Personal Computer Memory Card International Association*, e é usado como termo coletivo para todo o hardware e software relacionado.

19.1 Hardware

O componente mais importante é a placa PCMCIA. Existem dois tipos de placa PCMCIA:

Placas PC
: Essas placas existem desde o surgimento do padrão PCMCIA. Elas usam um barramento de 16 bits para a transmissão de dados e geralmente são muito baratas. Algumas pontes PCMCIA modernas têm dificuldade para detectar essas placas. No entanto, uma vez detectadas, elas geralmente funcionam bem e sem problemas.

Placas CardBus
: Esse é um padrão mais recente. Essas placas usam um barramento de 32 bits, o que as torna mais rápidas, porém mais caras também. Elas são integradas ao sistema como placas PCI e também apresentam um bom funcionamento.

O segundo componente importante é a controladora PCMCIA, ou a placa PC ou ponte CardBus, que estabelece a conexão entre a placa e o barramento PCI. Todos os modelos comuns são suportados. No caso de um dispositivo PCI interno, o comando `lspci -vt` fornece informações adicionais.

19.2 Software

Com o kernel atual, as pontes e placas PCMCIA são gerenciadas pelo subsistema de hotplug. Existem eventos `pcmcia_socket` para cada ponte e eventos `pcmcia`. udevd carrega todos os módulos necessários e chama as ferramentas requeridas para configurar esses dispositivos. Essas ações são definidas em `/etc/udev/rules.d/`.

`/etc/pcmcia/config.opts` é usado para a configuração de recursos. O driver necessário é determinado pelas tabelas do dispositivo nos drivers. Informações sobre o estado atual dos soquetes e das placas podem ser encontradas em `/sys/class/pcmcia_socket/` e usando-se `pccardctl`.

Uma vez que existem mudanças em andamento no sistema PCMCIA, esta documentação não é completa. Para obter uma visão geral mais abrangente, consulte `/usr/share/doc/packages/pcmciautils/README.SUSE`.

System Configuration Profile Management

20

Com a ajuda do SCPM (System Configuration Profile Management - Gerenciamento de Perfil da Configuração do Sistema) adapte a configuração do seu computador a diferentes ambientes operacionais ou configurações de hardware. O SCPM gerencia um conjunto de perfis do sistema para os diferentes cenários. O SCPM permite alternar facilmente entre perfis do sistema, eliminando a necessidade de reconfigurar manualmente o sistema.

Algumas situações requerem uma configuração do sistema modificada. Isso seria em geral o caso para computadores móveis que são operados em locais variáveis. O SCPM é prático se um sistema do desktop deve ser operado temporariamente usando componentes de hardware diferentes dos normais. A restauração da configuração do sistema original deve ser fácil e a modificação da configuração do sistema pode ser reproduzida. Com o SCPM, qualquer parte da configuração do sistema pode ser mantida em um perfil personalizado.

O campo principal de aplicação do SCPM é a configuração de rede em laptops. Configurações de rede diferentes geralmente requerem configurações diferentes de outros serviços, como e-mail ou proxies. Depois disso, vêm outros elementos, como impressoras diferentes em casa e no escritório, uma configuração personalizada de servidor X para o projetor multimídia em conferências, configurações especiais de economia de energia para viagens ou um fuso horário diferente em uma subsidiária estrangeira.

20.1 Terminologia

A seguir, estão alguns termos usados na documentação do SCPM e no módulo YaST.

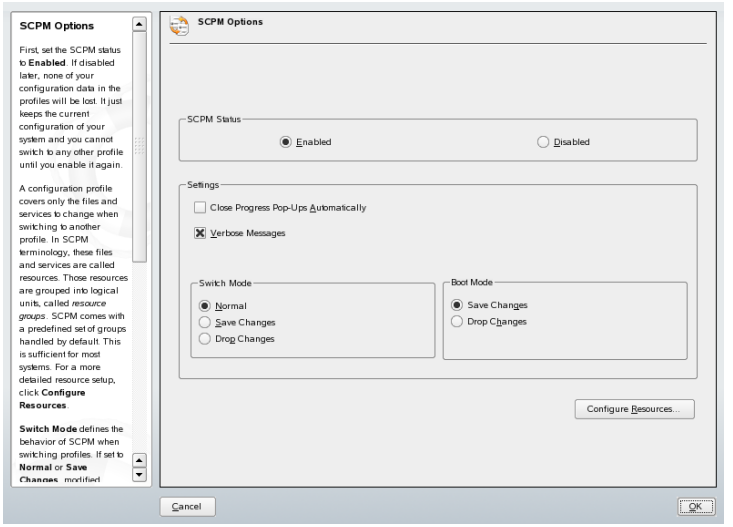
- O termo *configuração do sistema* refere-se à configuração completa do computador. Ele abrange todas as configurações fundamentais, como o uso de partições de disco rígido, configurações de rede, seleção de fuso horário e mapeamentos de teclado.
- Um *perfil*, também chamado de *perfil de configuração*, é um estado que foi preservado e que pode ser restaurado a qualquer momento.
- *Perfil ativo* refere-se ao perfil que foi selecionado por último. Isso não significa que a configuração do sistema atual corresponde exatamente a este perfil, porque ela pode ser modificada a qualquer momento.
- Um *recurso* no contexto do SCPM é um elemento que contribui para a configuração do sistema. Pode se tratar de um arquivo ou um softlink que inclua metadados (como o usuário), permissões ou tempo de acesso. Também pode ser um serviço do sistema que é executado neste perfil, mas está desabilitado em outro.
- Cada recurso pertence a um determinado *grupo de recursos*. Esses grupos contêm todos os recursos que logicamente devem estar juntos. A maioria de grupos conteria um serviço e seus arquivos de configuração. É muito fácil agrupar recursos gerenciados pelo SCPM porque isso não requer nenhum conhecimento dos arquivos de configuração do serviço desejado. O SCPM é fornecido com uma seleção de grupos de recursos pré-configurados que devem ser suficientes para a maioria dos cenários.

20.2 Usando o Gerenciador de Perfis do YaST

Inicie o gerenciador de perfis do YaST a partir do centro de controle do YaST com *Sistema* → *Gerenciador de Perfis*. Ao iniciar pela primeira vez, habilite explicitamente o SCPM selecionando *Habilitado* na caixa de diálogo *Opções do SCPM*, mostrada na Figura 20.1, “Opções do SCPM do YaST” (p 267). Em *Configurações*, determine se os popups de progresso devem ser fechados automaticamente e se devem ser exibidas mensagens com detalhes sobre o progresso da sua configuração do SCPM. Para *Modo*

de Troca, determine se os recursos modificados do perfil ativo devem ser gravados ou descartados quando o perfil é alternado. Se *Modo de Troca* estiver definido para *Normal*, todas as mudanças no perfil ativo serão gravadas quando ele for alternado. Para definir o comportamento do SCPM no momento da inicialização, defina *Modo de Boot* para *Salvar Mudanças* (configuração padrão) ou para *Descartar Mudanças*.

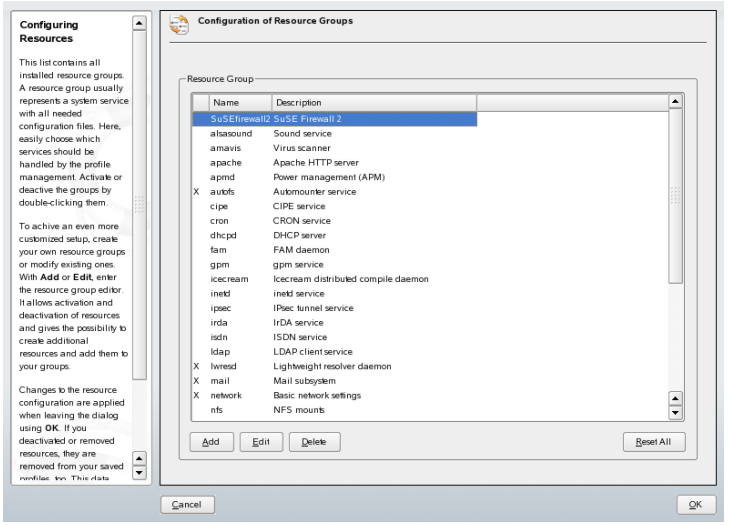
Figura 20.1 *Opções do SCPM do YaST*


SCPM Options
First, set the SCPM status to Enabled. If disabled later, none of your configuration data in the profiles will be lost. It just keeps the current configuration of your system and you cannot switch to any other profile until you enable it again.
A configuration profile covers only the files and services to change when switching to another profile. In SCPM terminology, these files and services are called resources. Those resources are grouped into logical units, called resource groups. SCPM comes with a predefined set of groups handled by default. This is sufficient for most systems. For a more detailed resource setup, click Configure Resources.
Switch Mode defines the behavior of SCPM when switching profiles. If set to Normal or Save Changes, modified
SCPM Options
SCPM Status
Enabled
Disabled
Settings
Close Progress Pop-Ups Automatically
Verbose Messages
Switch Mode
Normal
Save Changes
Drop Changes
Boot Mode
Save Changes
Drop Changes
Configure Resources...
Cancel
OK

20.2.1 Configurando grupos de recursos

Para fazer mudanças na configuração de recursos atual, escolha *Configurar Recursos* na caixa de diálogo *Opções do SCPM*. A próxima caixa de diálogo, mostrada na Figura 20.2, “Configurando grupos de recursos” (p 268), relaciona todos os grupos de recursos disponíveis no seu sistema. Para adicionar ou editar um grupo de recursos, especifique ou modifique *Grupo de Recursos* e *Descrição*. Para um serviço LDAP, por exemplo, digite `ldap` como *Grupo de Recursos* e `Serviço de cliente LDAP` como *Descrição*. Digite então os recursos apropriados (serviços, arquivos de configuração ou ambos) ou modifique os existentes. Apague aqueles que não são usados. Para redefinir o status dos recursos selecionados (descarte quaisquer mudanças feitas a eles e retorne aos valores de configuração iniciais), escolha *Reconfigurar Grupo*. Suas mudanças são gravadas no perfil ativo.

Figura 20.2 *Configurando grupos de recursos*

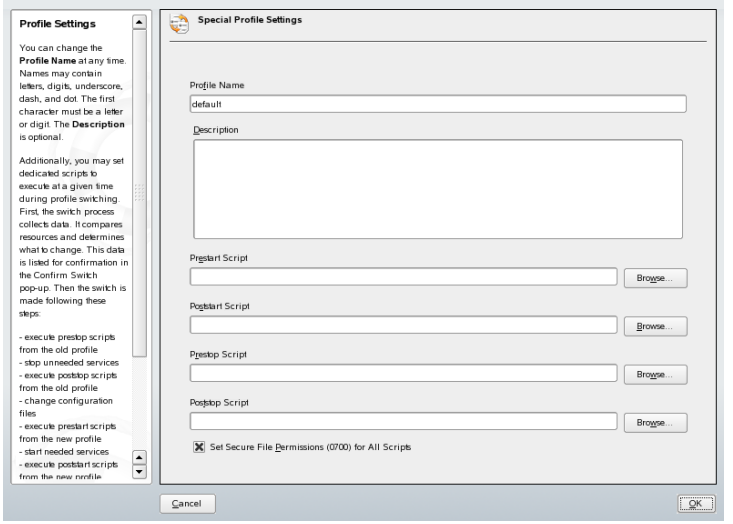

Configuring Resources
This list contains all installed resource groups. A resource group usually represents a system service with all needed configuration files. Here, easily choose which services should be handled by the profile management. Activate or deactive the groups by double-clicking them.
To achive an even more customized setup, create your own resource groups or modify existing ones. With Add or Edit, enter the resource group editor. It allows activation and deactivation of resources and gives the possibility to create additional resources and add them to your groups.
Changes to the resource configuration are applied when leaving the dialog using OK. If you deactivated or removed resources, they are removed from your saved
Configuration of Resource Groups
Resource Group
Name
Description
SuSEfirewall2 SuSE Firewall 2
alsasound Sound service
amavis Virus scanner
apache Apache HTTP server
apmd Power management (APM)
X autofs Automounter service
cipe CIPE service
cron CRON service
dhcpd DHCP server
fam FAM daemon
gpm gpm service
icecream Icecream distributed compile daemon
inetd inetd service
ipsec IPsec tunnel service
irda IrDA service
isdn ISDN service
ldap LDAP client service
X lwresd Lightweight resolver daemon
X mail Mail subsystem
X network Basic network settings
nfs NFS mounts
Add
Edit
Delete
Reset All
Cancel
OK

20.2.2 Criando um novo perfil

Para criar um novo perfil, clique em *Adicionar* na caixa de diálogo de início (*System Configuration Profile Management*). Na janela que será aberta, selecione se o novo perfil deve ser baseado na configuração do sistema atual (o SCPM recupera automaticamente a configuração atual e a grava no seu perfil) ou em um perfil existente. Se você usar a configuração do sistema atual como a base do novo perfil, poderá marcar o novo perfil como o novo perfil ativo. Isso não faz mudanças no perfil antigo e não inicia nem interrompe os serviços.

Forneça um nome e uma breve descrição para o novo perfil na caixa de diálogo a seguir. Para que o SCPM execute scripts especiais em uma alternação de perfis, digite os caminhos de cada executável (consulte a Figura 20.3, “Configurações de perfil especiais” (p 269)). Consulte a Seção 20.3.4, “Configurações avançadas de perfil” (p 272) para obter mais informações. O SCPM executa uma verificação para os recursos do novo perfil. Depois que este teste foi concluído com sucesso, o novo perfil estará pronto para ser usado.

Figura 20.3 *Configurações de perfil especiais*


Profile Settings
You can change the Profile Name at any time. Names may contain letters, digits, underscore, dash, and dot. The first character must be a letter or digit. The Description is optional.
Additionally, you may set dedicated scripts to execute at a given time during profile switching. First, the switch process collects data. It compares resources and determines what to change. This data is listed for confirmation in the Confirm Switch pop-up. Then the switch is made following these steps:
- execute prestop scripts from the old profile
- stop unneeded services
- execute poststop scripts from the old profile
- change configuration files
- execute prestart scripts from the new profile
- start needed services
- execute poststart scripts
Special Profile Settings
Profile Name
default
Description
Prestart Script
Browse...
Poststart Script
Browse...
Prestop Script
Browse...
Poststop Script
Browse...
Set Secure File Permissions (0700) for All Scripts
Cancel
OK

20.2.3 Modificando perfis existentes

Para modificar um perfil existente, escolha *Editar* na caixa de diálogo de início (*System Configuration Profile Management*). Em seguida, modifique o nome, a descrição, os scripts e os recursos de acordo com as suas necessidades.

20.2.4 Alternando perfis

Para alternar perfis, abra o gerenciador de perfis. O perfil ativo é marcado com uma seta. Selecione o perfil para o qual alternar e clique em *Trocar para*. O SCPM verifica recursos novos ou modificados e os adiciona, se necessário.

Se um recurso foi modificado, o YaST abre a caixa de diálogo *Confirmar Troca*. *Grupos de Recurso do Perfil Ativo Modificados* relaciona todos os grupos de recursos do perfil ativo que foram modificados, mas que ainda não foram salvos no perfil ativo. *Gravar ou Ignorar* para o grupo de recursos selecionado atualmente determina se as mudanças feitas nesse grupo de recursos devem ser gravadas no perfil ativo ou descartadas. Alternativamente, selecione cada recurso e clique em *Detalhes* para analisar as mudanças em detalhes. Isso mostra uma lista de todos os arquivos de configuração ou executáveis

pertencentes a esse grupo de recursos que foram modificados. Para obter uma comparação linha por linha entre a versão antiga e a nova, clique em *Mostrar Modificações*. Após analisar as mudanças, decida o que fazer com elas em *Ação*:

Salvar Recurso
Grava este recurso no perfil ativo, mas deixa todos os outros perfis intactos.

Ignorar Recurso
Deixa o recurso ativo intacto. Essa mudança é descartada.

Salvar em Todos os Perfis
Copia a configuração inteira deste recurso para todos os outros recursos.

Fazer Patch em todos os Perfis
Aplica somente as mudanças mais recentes a todos os perfis.

Salvar ou Ignorar Todos simplesmente grava ou descarta as mudanças de todos os recursos mostrados nesta caixa de diálogo.

Após confirmar as mudanças no perfil ativo, saia da caixa de diálogo *Confirmar Troca* clicando em *OK*. O SCPM alterna para o novo perfil. Ao alternar, ele executa os scripts pré-parar e pós-parar do perfil antigo e os scripts pré-início e pós-início do novo perfil.

20.3 Configurando o SCPM com a linha de comando

Esta seção introduz a configuração de linha de comando do SCPM. Aprenda como iniciá-la, configurá-la e trabalhar com perfis.

20.3.1 Iniciando o SCPM e definindo grupos de recursos

O SCPM deve ser ativado antes de ser usado. Ative o SCPM com `scpm enable`. Ao ser executado pela primeira vez, o SCPM é inicializado, o que leva alguns segundos. Desative o SCPM com `scpm disable` a qualquer momento para evitar a troca não intencional de perfis. Uma reativação subseqüente simplesmente reinicia a inicialização.

Por padrão, o SCPM trata configurações de rede e impressora, assim como a configuração X.Org. Para gerenciar serviços ou arquivos de configuração especiais, ative os grupos de recursos respectivos. Para relacionar os grupos de recursos predefinidos, use `scpm list_groups`. Para ver somente os grupos já ativados, use `scpm list_groups -a`. Emita estes comandos como `root` na linha de comando.

```
scpm list_groups -a

nis                 Network Information Service client
mail                Mail subsystem
ntpd                Network Time Protocol daemon
xf86                X Server settings
autofs              Automounter service
network             Basic network settings
printer             Printer settings
```

Ative ou desative um grupo com `scpm activate_group NOME` ou `scpm deactivate_group NOME`. Substitua `NOME` pelo nome de grupo relevante.

20.3.2 Criando e gerenciando perfis

Um perfil chamado `default` já existe depois que o SCPM foi ativado. Obtenha uma lista de todos os perfis disponíveis com `scpm list`. Este perfil existente também é o perfil ativo, que pode ser verificado com `scpm active`. O perfil `default` é uma configuração básica da qual os outros perfis são derivados. Por este motivo, todas as configurações que devem ser idênticas em todos os perfis devem ser criadas primeiro. Em seguida, armazene essas modificações no perfil ativo com `scpm reload`. O perfil `default` pode ser copiado e renomeado como a base de novos perfis.

Existem duas maneiras de adicionar um novo perfil. Se o novo perfil (chamado `trabalho` aqui) deve ser baseado no perfil `default`, crie-o com `scpm copy default trabalho`. O comando `scpm switch trabalho` muda para o novo perfil, que pode então ser modificado. Convém modificar a configuração do sistema para finalidades especiais e gravar as mudanças em um novo perfil. O comando `scpm add trabalho` cria um novo perfil gravando a configuração do sistema atual no perfil `trabalho` e tornando-a ativa. A execução de `scpm reload` grava as mudanças no perfil `trabalho`.

Os perfis podem ser renomeados ou apagados com os comandos `scpm rename x y` e `scpm delete z`. Por exemplo, para renomear `trabalho` para `projeto`, digite

`scpm rename trabalho projeto`. Para apagar `projeto`, digite `scpm delete projeto`. O perfil ativo não pode ser apagado.

20.3.3 Alternando perfis de configuração

O comando `scpm switch trabalho` alterna para um outro perfil (o perfil `trabalho`, neste caso). Alterne para o perfil ativo a fim de incluir configurações modificadas da configuração do sistema no perfil. Isso corresponde ao comando `scpm reload`.

Ao alternar perfis, o SCPM primeiro verifica que recursos do perfil ativo foram modificados. Em seguida, ele consulta se a modificação de cada recurso deve ser adicionada ao perfil ativo ou descartada. Se você preferir ter uma lista separada de recursos (como em versões antigas do SCPM), use o comando de troca com o parâmetro `–r`: `scpm switch –r trabalho`.

```
scpm switch –r trabalho

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

O SCPM compara então a configuração do sistema atual com o perfil para o qual alternar. Nesta fase, o SCPM avalia que serviços do sistema precisam ser interrompidos ou reiniciados devido a dependências mútuas ou a fim de refletir as mudanças na configuração. Isso é como uma reinicialização parcial do sistema que somente afeta uma pequena parte do sistema enquanto o resto continua operando sem mudanças. É somente neste ponto que os serviços do sistema são interrompidos, todos os recursos modificados, como arquivos de configuração, são gravados, e os serviços do sistema são reiniciados.

20.3.4 Configurações avançadas de perfil

Você pode digitar uma descrição para cada perfil que é exibido com `scpm list`. Para o perfil ativo, defina-o com `scpm set description "texto"`. Forneça o nome do perfil para perfis inativos, por exemplo, `scpm set description "texto" trabalho`. Talvez convenha, algumas vezes, executar ações adicionais não fornecidas pelo SCPM ao alternar perfis. Anexe de um a quatro executáveis para cada perfil. Eles

são chamados em estágios diferentes do processo de alternação. Estes estágios são conhecidos como:

pré-parar
antes de interromper serviços ao deixar o perfil

pós-parar
após interromper serviços ao deixar o perfil

pré-iniciar
antes de iniciar serviços ao ativar o perfil

pós-iniciar
após iniciar serviços ao ativar os perfis

Insira estas ações com o comando `set` digitando `scpm set pré-parar filename`, `scpm set pós-parar filename`, `scpm set pré-iniciar filename` ou `scpm set pós-iniciar filename`. Os scripts devem ser executáveis e devem indicar o interpretador correto.

ATENÇÃO: Integrando um script personalizado

Os scripts adicionais a serem executados pelo SCPM devem ser legíveis e executáveis para o superusuário (`root`). O acesso a esses arquivos deve ser bloqueado para todos os usuários. Digite os comandos `chmod 700 filename` e `chown root:root filename` para dar ao `root` permissões exclusivas aos arquivos.

Consulte todas as configurações adicionais digitadas com `set` com `get`. O comando `scpm get pós-iniciar`, por exemplo, retorna o nome da chamada pós-iniciar ou simplesmente nada se nada foi anexado. Redefina essas configurações subregravando com `""`. O comando `scpm set pré-parar ""` remove o programa pré-parar anexado.

Todos os comandos `set` e `get` podem ser aplicados a um perfil arbitrário da mesma maneira que os comentários são adicionados. Por exemplo, `scpm get pré-parar filename trabalho` ou `scpm get pré-parar trabalho`.

20.4 Usando o applet Seletor de Perfil

O applet Seletor de Perfil no seu painel da área de trabalho do GNOME ou KDE permite controlar facilmente suas configurações SCPM. Crie, modifique ou apague perfis através do YaST conforme descrito na Seção 20.2, “Usando o Gerenciador de Perfis do YaST” (p 266) e alterne perfis. Você pode alternar perfis como usuário normal desde que o administrador do sistema permita que isso ocorra. Inicie o Seletor de Perfil a partir do seu menu da área de trabalho usando *Sistema → Applet de Desktop → Seletor de Perfil*.

Permita que os usuários normais alternem perfis clicando o botão direito do mouse no ícone Seletor de Perfil no painel da área de trabalho e escolhendo *Permitir alternar por usuários não-raiz* no menu que abre. Forneça a senha do root. Qualquer usuário autorizado no seu sistema pode alternar perfis de agora em diante.

Todos os perfis configurados no YaST, diretamente através de uma chamada do YaST ou através de *Iniciar Módulo de Gerenciamento de Perfil do YaST2* são exibidos depois que você clica no ícone Seletor de Perfil. Selecione o perfil para o qual alternar usando as teclas do cursor e as mudanças do SCPM ao novo perfil automaticamente.

20.5 Solução de problemas

Esta seção abrange problemas freqüentes encontrados com o SCPM. Aprenda como eles podem ocorrer e como você pode resolvê-los.

20.5.1 Encerramento durante o processo de alternação

Às vezes, o SCPM pára de funcionar durante um procedimento de alternação. Isso pode ser causado por algum efeito externo, como uma interrupção do usuário, uma falha de energia ou mesmo um erro no próprio SCPM. Se isso ocorrer, uma mensagem de erro que declara que o SCPM está bloqueado será exibida na próxima vez que você iniciar o SCPM. Isso é para a segurança do sistema, pois os dados armazenados no seu banco de dados talvez sejam diferentes do estado do sistema. Para resolver essa questão, execute `scpm recover`. O SCPM executa todas as operações ausentes da execução

anterior. Você também pode executar `scpm recover -b`, que tenta desfazer todas as operações já executadas da execução anterior. Se estiver usando o gerenciador de perfis do YaST, obtenha uma caixa de diálogo de recuperação na inicialização que oferece a execução dos comandos descritos acima.

20.5.2 Mudando a configuração do grupo de recursos

Para modificar a configuração do grupo de recursos quando o SCPM já foi inicializado, digite `scpm rebuild` após adicionar ou remover grupos. Dessa forma, novos recursos são adicionados a todos os perfis e os recursos removidos são apagados permanentemente. Se os recursos apagados forem configurados de forma diferente nos vários perfis, esses dados de configuração serão perdidos, exceto para a versão atual no seu sistema, que o SCPM deixa intacta. Se você modificar a configuração com o YaST, o comando de reconstrução não precisará ser digitado, pois isso é tratado pelo YaST.

20.6 Selecionando um perfil ao inicializar o sistema

Para selecionar um perfil ao inicializar o sistema, pressione F3 na tela de inicialização para acessar uma lista de perfis disponíveis. Use as teclas de seta para selecionar um perfil e confirmar sua seleção com Enter. O perfil selecionado é então usado como uma opção de inicialização.

20.7 Mais informações

A documentação mais recente está disponível nas páginas de informações do SCPM (info scpm). As informações para desenvolvedores estão disponíveis em `/usr/share/doc/packages/scpm`.

21 Gerenciamento de energia

O gerenciamento de energia é especialmente importante em laptops, mas também é útil em outros sistemas. Duas tecnologias estão disponíveis: APM (Advanced Power Management - Gerenciamento Avançado Energia) e ACPI (Advanced Configuration and Power Interface - Interface de Energia e Configuração Avançada). Além delas, também é possível controlar o dimensionamento de freqüência de CPU para economizar energia ou reduzir o ruído. Estas opções podem ser configuradas manualmente ou usando um módulo YaST especial.

Ao contrário de APM, que era usado em laptops apenas para gerenciamento de energia, a ferramenta ACPI de configuração e informações sobre hardware está disponível em todos os computadores modernos (laptops, desktops e servidores). Todas as tecnologias de gerenciamento de energia exigem hardware adequado e rotinas BIOS. A maioria dos laptops e muitas áreas de trabalho e servidores modernos atendem a estes requisitos.

APM era usado em muitos computadores antigos. Como APM consiste amplamente em um conjunto de funções implementado no BIOS, o nível de suporte de APM pode variar, dependendo do hardware. O mesmo vale para o ACPI, que é ainda mais complexo. Por esta razão, é virtualmente impossível recomendar um ou outro. Teste os diversos procedimentos no seu hardware e selecione a tecnologia que é suportada de forma melhor.

IMPORTANTE: Gerenciamento de energia para processadores AMD64

Processadores AMD64 com kernel de 64 bits suportam apenas o ACPI.

21.1 Funções de economia de energia

As funções de economia de energia não são significativas apenas para o uso móvel de laptops, como também para sistemas desktop. As principais funções e uso respectivo nos sistemas de gerenciamento de energia APM e ACPI são:

Standby
Este modo operacional desativa a exibição. Em alguns computadores, o desempenho do processador é restringido. Essa função não está disponível em todas as implementações do APM. Ela corresponde ao estado S1 ou S2 da ACPI.

Suspender (para memória)
Este modo grava todo o estado do sistema na memória RAM. Em seguida, todo o sistema é colocado para adormecer, salvo a memória RAM. Neste estado, o computador consome pouquíssima energia. A vantagem desse estado é a possibilidade de reiniciar o trabalho no mesmo ponto em alguns segundos sem precisar inicializar e reiniciar os aplicativos. Dispositivos que usam APM geralmente podem ser suspensos fechando-se a tampa e ativados abrindo-a. Esta função corresponde ao estado S3 de ACPI. O suporte desse estado ainda está em desenvolvimento e, portanto, depende muito do hardware.

Suspender (para o disco)
Neste modo operacional, o estado do sistema inteiro é gravado no disco rígido e o sistema é desligado. A reativação desse estado leva de 30 a 90 segundos. O estado anterior ao suspenso é restaurado. Alguns fabricantes oferecem variantes híbridas desse modo, como RediSafe em Thinkpads da IBM. O estado correspondente da ACPI é S4. No Linux, suspender para disco é realizado pelas rotinas kernel que são independentes de APM e ACPI.

Monitor de bateria
ACPI e APM verificam o status da carga da bateria e fornecem informações sobre o status da carga. Além disso, os dois sistemas coordenam ações a realizar quando um status de carga é atingido.

Desligamento automático
Após um encerramento, o computador é desligado. Isto é especialmente importante quando um encerramento automático é realizado pouco antes da bateria esgotar-se.

Encerramento dos componentes do sistema
Desativar o disco rígido é o principal aspecto do potencial de economia de energia de todo o sistema. Dependendo da confiabilidade do sistema, o disco rígido pode ser colocado para adormecer por algum tempo. No entanto, o risco de perder dados aumenta com a duração dos períodos de adormecimento. Outros componentes podem ser desativados por meio de ACPI (pelo menos em teoria) ou permanentemente na configuração do BIOS.

Controle de velocidade do processador
Junto com a CPU, é possível economizar energia de três maneiras: escala de freqüência e voltagem (também conhecida como PowerNow! ou Speedstep), obstruindo e colocando o processador para adormecer (estados C). Dependendo do modo operacional do computador, esses métodos também podem ser combinados.

21.2 APM

Algumas das funções de economia de energia são realizadas pelo próprio BIOS do APM. Em muitos laptops, os estados standby e suspender podem ser ativados com combinações de tecla ou fechando a tampa sem qualquer função especial do sistema operacional. No entanto, para ativar esses modos com um comando, algumas ações devem ser acionadas antes que o sistema seja suspenso. Para visualizar o nível de carga da bateria, são necessários pacotes especiais de programa e um kernel adequado.

Os kernels do SUSE Linux têm suporte de APM interno. No entanto, APM só é ativado se ACPI não estiver implementada no BIOS e for detectado um BIOS de APM. Para ativar o suporte APM, ACPI deve ser desativado com `acpi=off` no prompt de inicialização. Digite `cat /proc/apm` para verificar se APM está ativo. Uma saída composta de vários números indica que tudo está OK. Você agora poderá desligar o computador com o comando `shutdown -h`.

As implementações do BIOS que não forem totalmente compatíveis com o padrão poderão provocar problemas com APM. Alguns problemas poderão ser contornados com parâmetros de boot especiais. Todos os parâmetros são gravados no prompt de inicialização no formato `apm=parameter`:

ativar ou desativar
Habilitar ou desabilitar suporte APM.

(no-)allow-ints
Permitir interrupções durante a execução das funções do BIOS

(no-)broken-psr
A função “GetPowerStatus” do BIOS não funciona corretamente.

(no-)realmode-power-off
Redefina o processador para o modo real antes de desligar.

(no-)debug
Registre os eventos APM no registro do sistema.

(no-)realmode-power-off
Desligue o sistema após o encerramento.

bounce-interval=*n*
Tempo em centésimos de segundo após um evento suspenso durante o qual os eventos suspensos adicionais são ignorados.

idle-threshold=*n*
Porcentagem de inatividade do sistema na qual a função do BIOS `idle` é executada (0=sempre, 100=nunca).

idle-period=*n*
Tempo em centésimos de segundo após o qual a atividade do sistema é medida.

O daemon APM (apmd) não é mais usado. A sua funcionalidade agora é tratada pela nova economia de energia, que também aceita dimensionamento de freqüência de ACPI e CPU.

21.3 ACPI

A ACPI (Interface de Energia e Configuração Avançada) foi projetada para habilitar o sistema operacional a configurar e controlar os componentes individuais do hardware. A ACPI substitui PnP e APM. Envia informações sobre a bateria, adaptador de CA, temperatura, ventilador e eventos do sistema, como “fechar tampa” ou “bateria fraca.”

O BIOS fornece tabelas que contém informações sobre os componentes individuais e métodos de acesso ao hardware. O sistema operacional usa essas informações para

tarefas como atribuir interrupções ou ativar e desativar componentes. Como o sistema operacional executa comandos armazenados no BIOS, a funcionalidade depende da implementação do BIOS. As tabelas que a ACPI podem detectar e carregar são reportadas em `/var/log/boot.msg`. Consulte Seção 21.3.4, “Solução de problemas” (p 286) para obter mais informações sobre solução de problemas da ACPI.

21.3.1 ACPI em ação

Se o kernel detectar um BIOS de ACPI quando o sistema for inicializado, a ACPI será automaticamente ativada e o APM desativado. O parâmetro de inicialização `acpi=force` poderá ser necessário para algumas máquinas mais antigas. O computador deve aceitar ACPI 2.0 ou posterior. Verifique as mensagens de boot do kernel em `/var/log/boot.msg` para ver se a ACPI foi ativada.

Em seguida, deverá ser carregado um número de módulos. Isso é feito pelo script de início do daemon de economia de energia. Se algum destes módulos causar problemas, o módulo respectivo poderá ser excluído de carregar ou descarregar em `/etc/sysconfig/powersave/common`. O registro do sistema (`/var/log/messages`) contém as mensagens dos módulos, permitindo que você veja que componentes foram detectados.

`/proc/acpi` agora contém vários arquivos que fornecem informações sobre o estado do sistema ou que podem ser usados para mudar alguns dos estados. Alguns recursos ainda não funcionam porque estão em desenvolvimento e o suporte de algumas funções depende muito da implementação do fabricante.

Todos os arquivos (exceto `dsdt` e `fadt`) podem ser lidos com `cat`. Em alguns arquivos, as configurações podem ser modificadas com `echo`, por exemplo, `echo X > file` para especificar valores adequados para X. Use sempre o comando `powersave` para acessar estas informações e as opções de controle. Os arquivos mais importantes estão descritos abaixo:

`/proc/acpi/info`
Informações gerais sobre a ACPI.

`/proc/acpi/alarm`
Aqui, especifique quando o sistema deve ser ativado de um estado de inatividade. Atualmente, esse recurso não é totalmente suportado.

/proc/acpi/sleep
Fornece informações sobre possíveis estados de adormecimento.

/proc/acpi/event
Todos os eventos são reportados aqui e processados pelo daemon do Powersave (`powersaved`). Se nenhum daemon acessar o arquivo, eventos como um clique rápido no botão de alimentação ou fechamento da tampa podem ser lidos com `cat /proc/acpi/event` (encerrar com Ctrl + C).

/proc/acpi/dsdt e /proc/acpi/fadt
Estes arquivos contêm as tabelas DSDT (differentiated system description table - tabela de descrição de sistema diferenciado) e FADT (fixed ACPI description table - tabela de descrição de ACPI fixa) da ACPI. Elas podem ser lidas com `acpidmp`, `acpidisasm` e `dmdecode`. Estes programas e sua documentação localizam-se no `pmtools do pacote`. Por exemplo, `acpidmp DSDT | acpidisasm`.

/proc/acpi/ac_adapter/AC/state
Mostra se o adaptador de CA está conectado.

/proc/acpi/battery/BAT*/{alarme,info,estado}
Informações detalhadas sobre o estado da bateria. O nível de carga é lido através da comparação da `última capacidade cheia` e `info` com a `capacidade remanescente` no `estado`. Um modo mais confortável de fazer isto é usar um dos programas especiais apresentados em Seção 21.3.3, “Ferramentas da ACPI” (p 286). O nível de carga em que o evento bateria é acionado pode ser especificado em `alarme`.

/proc/acpi/button
Este diretório contém informações sobre vários switches.

/proc/acpi/fan/FAN/state
Mostra se o ventilador está ativo atualmente. Ativar ou desativar o ventilador manualmente, escrevendo `0` (ligado) ou `3` (desligado) neste arquivo. No entanto, os dois códigos da ACPI no kernel e no hardware (ou no BIOS) sobregravam esta configuração no caso de aquecimento.

/proc/acpi/processor/*
É mantido um subdiretório separado para cada CPU incluída no seu sistema.

/proc/acpi/processor/*/info
Informações sobre as opções de economia de energia do processador.

/proc/acpi/processor/*/power
Informações sobre o estado atual do processador. Um asterisco próximo a `C2` indica que o processador está inativo. Este é o estado mais freqüente, como pode ser verificado no valor de `utilizaç o`.

/proc/acpi/processor/*/throttling
Pode ser usado para configurar o throttling do relógio do processador. Normalmente, é possível o throttling em oito níveis. Isto é independente do controle de freqüência da CPU.

/proc/acpi/processor/*/limit
Se o desempenho (desatualizado) e o throttling forem controlados automaticamente por um daemon, os limites máximos podem ser especificados aqui. Alguns dos limites são determinados pelo sistema. Alguns podem ser ajustados pelo usuário.

/proc/acpi/thermal_zone/
Existe um subdiretório separado para cada zona térmica. Uma zona térmica é uma área com propriedades térmicas similares, cujo número e nomes são designados pelo fabricante do hardware. No entanto, muitas das possibilidades oferecidas pela ACPI raramente são implementadas. Ao contrário, o controle de temperatura convencionalmente é administrado pelo BIOS. O sistema operacional não tem muita oportunidade de intervir, porque a vida útil do hardware está ameaçada. Portanto, alguns dos arquivos têm apenas um valor teórico.

/proc/acpi/thermal_zone/*/temperature
Temperatura atual da zona térmica.

/proc/acpi/thermal_zone/
O estado indica se tudo está `ok` ou se a ACPI aplica o resfriamento `ativo` ou `passivo`. No caso de controle de ventilador independente da ACPI, o estado está sempre `ok`.

/proc/acpi/thermal_zone/*/cooling_mode
Selecione o método de resfriamento controlado pela ACPI Escolha o modo de resfriamento passivo (menor desempenho, econômico) ou ativo (total desempenho, ruído do ventilador).

/proc/acpi/thermal_zone/*/trip_points
: Habilita a determinação de limites de temperatura para acionamento de ações específicas, como resfriamento ativo ou passivo, suspensão (`quente`), ou um shutdown (`crítico`). As ações possíveis são definidas no DSDT (dependente do dispositivo). Os pontos de desligamento determinados na especificação da ACPI são `crítico`, `quente`, `passivo`, `ativo1` e `ativo2`. Mesmo que nem todos eles sejam implementados, devem ser sempre digitados neste arquivo nesta ordem. Por exemplo, a entrada `echo 90:0:70:0:0 > trip_points` configura a temperatura de `crítico` a `90` e a temperatura de `passivo` a `70` (todas as temperaturas medidas em graus Celsius).

/proc/acpi/thermal_zone/*/polling_frequency
: Se o valor em `temperatura` não for atualizado automaticamente quando a temperatura mudar, alterne o modo polling aqui. Com o comando `echo X > /proc/acpi/thermal_zone/*/polling_frequency` a temperatura é verificada a cada `X` segundos. Configure `X=0` para desabilitar o polling.

Nenhuma destas configurações, informações e eventos precisam ser editados manualmente. Isto pode ser feito com o daemon do Powersave (economia de energia) e diversos aplicativos, como powersave, kpowersave e wmpowersave. Consulte Seção 21.3.3, “Ferramentas da ACPI” (p 286). Como powersaved cobre as funcionalidades do acpid antigo, acpid não é mais necessário.

21.3.2 Controlando o desempenho da CPU

A CPU pode economizar energia de três maneiras. Dependendo do modo operacional do computador, estes métodos também podem ser combinados. Economizar energia também significa que o sistema esquenta menos e os ventiladores são ativados com menos freqüência.

Dimensionamento de freqüência e voltagem
: PowerNow! e Speedstep são as designações de uso AMD e Intel para esta tecnologia. No entanto, essa tecnologia também é aplicada em processadores de outros fabricantes. A freqüência do relógio da CPU e sua voltagem básica são reduzidas ao mesmo tempo, resultando em economias de energia mais do que lineares. Isso significa que quando a freqüência for reduzida pela metade (meio desempenho), muito menos que metade da energia é consumida. Essa tecnologia é independente de APM e ACPI e exige um daemon que adapte a necessidade de freqüência e a

necessidade atual de desempenho. As configurações podem ser feitas no diretório `/sys/devices/system/cpu/cpu*/cpufreq/`.

Throttling da freqüência do relógio
Esta tecnologia omite uma determinada porcentagem dos impulsos de sinal do relógio para a CPU. Com throttling a 25%, todo quarto impulso é omitido. A 87,5%, apenas cada oitavo impulso chega ao processador. No entanto, as economias de energia são pouco menos que lineares. Normalmente, o throttling só é usado se o dimensionamento da freqüência não estiver disponível ou para maximizar as economias de energia. Essa tecnologia também deve ser controlada por um processo especial. A interface do sistema é `/proc/acpi/processor/*/throttling`.

Colocando o processador para hibernar
O sistema operacional coloca o processador para hibernar sempre que não houver nada para fazer. Neste caso, o sistema operacional envia um comando de `halt` para a CPU. Há três estados: C1, C2 e C3. No estado mais econômico, C3, até a sincronização do cache do processador com a memória principal é interrompida. Portanto, esse estado só pode ser aplicado se nenhum dispositivo modificar o conteúdo da memória principal por meio de atividade do barramento mestre. Alguns drivers impedem o uso de C3. O estado atual é exibido em `/proc/acpi/processor/*/power`.

O dimensionamento e o throttling da freqüência só são relevantes se o processador estiver ocupado, porque o estado C mais econômico é aplicado sempre que o processador está inativo. Se a CPU estiver ocupada, o dimensionamento da freqüência é o método recomendado para economia de energia. Em geral o processador só trabalha com carga parcial. Neste caso, pode ser executado com uma freqüência inferior. Normalmente, o dimensionamento dinâmico de freqüência controlado por um daemon, como powersaved, é o melhor método. Uma configuração estática em baixa freqüência é útil para operações a bateria ou se você desejar que o computador permaneça frio ou em silêncio.

Throttling deve ser usado como última alternativa, por exemplo, para ampliar o tempo de operação da bateria, apesar de uma alta carga do sistema. Contudo, alguns sistemas não são executados suavemente quando ocorrem throttlings em excesso. Ademais, o throttling da CPU não faz sentido se a CPU tem pouco a fazer.

No SUSE Linux estas tecnologias são controladas pelo daemon do powersave. A configuração está explicada em Seção 21.5, “O Pacote powersave” (p 289).

21.3.3 Ferramentas da ACPI

A faixa mais ou menos abrangente dos utilitários da ACPI inclui ferramentas que apenas exibem informações, como o nível de carga e a temperatura da bateria (acpi, klaptopdaemon, wmacpimon, etc.), ferramentas que facilitam o acesso às estruturas de `/proc/acpi` ou que auxiliam no monitoramento das mudanças (akpi, acpiw, gtkacpiw) e ferramentas para edição das tabelas da ACPI no BIOS (pacote `pmtools`).

21.3.4 Solução de problemas

Há dois tipos de problemas. De um lado, o código ACPI do kernel pode conter erros que não foram detectados em tempo útil. Neste caso, uma solução estará disponível para download. No entanto, o mais comum é que os problemas sejam causados pelo BIOS. Às vezes, desvios da especificação da ACPI são integrados de propósito no BIOS para contornar erros na implementação da ACPI em outros sistemas operacionais amplamente utilizados. Componentes de hardware que têm erros sérios na implementação da ACPI são gravados em uma lista negra que impede que o kernel do Linux use a ACPI para esses componentes.

A primeira ação a ser tomada quando problemas forem detectados, é atualizar o BIOS. Se o computador não inicializar de jeito nenhum, um dos seguintes parâmetros de inicialização poderá ser útil:

pci=noacpi
: Não use ACPI para configurar os dispositivos PCI.

acpi=oldboot
: Realize apenas uma configuração com recursos simples. Não use a ACPI para outros fins.

acpi=off
: Desabilitar a ACPI.

ATENÇÃO: Problemas de inicialização sem ACPI

Algumas máquinas mais novas (especialmente os sistemas SMP e AMD64) precisam de ACPI para configurar o hardware corretamente. Nestas máquinas, desabilitar a ACPI pode causar problemas.

Monitore as mensagens de inicialização do sistema com o comando `dmesg | grep -2i acpi` (ou todas as mensagens, porque o problema pode não ser causado pela ACPI) após a inicialização. Se ocorrer um erro ao analisar uma tabela da ACPI, a tabela mais importante, a DSDT, pode ser substituída por uma versão aperfeiçoada. Neste caso, a DSDT defeituosa do BIOS é ignorada. O procedimento está descrito em Seção 21.5.4, “Solução de problemas” (p 295).

Na configuração do kernel, há um switch para ativar as mensagens de depuração da ACPI. Se um kernel com depuração da ACPI for compilado e instalado, os técnicos que procuram o erro podem ser auxiliados com informações detalhadas.

Se você tiver problemas com BIOS ou hardware, é sempre recomendável entrar em contato com os fabricantes. Especialmente se eles nem sempre derem assistência ao Linux, devem ser indagados em caso de problemas. Os fabricantes só levarão a questão a sério se compreenderem que um número satisfatório de seus clientes usa Linux.

Para obter mais informações

Documentação adicional e suporte para a ACPI:

- `http://www.cpqlinux.com/acpi-howto.html` (ACPI HOWTO detalhado, contém patches DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (ACPI FAQ @Intel)
- `http://acpi.sourceforge.net/` (O projeto ACPI4Linux em Sourceforge)
- `http://www.poupinou.org/acpi/` (patches DSDT por Bruno Ducrot)

21.4 Descanso do disco rígido

No Linux, o disco rígido pode colocado em hibernação total se não estiver em uso e pode ser executado em modo mais econômico ou silencioso. Nos laptops modernos, não é necessário desativar o disco rígido manualmente, porque entram automaticamente em um modo operacional econômico sempre que não estão em uso. Contudo, se quiser maximizar a economia de energia, teste um dos seguintes métodos. A maioria das funções pode ser controlada com powersaved e o módulo de gerenciamento de energia

YaST, que é explicado em mais detalhes em Seção 21.6, “O módulo Gerenciamento de energia YaST” (p 297).

O aplicativo hdparm pode ser usado para modificar diversas configurações do disco rígido. A opção `-y` alterna instantaneamente o disco rígido para o modo standby. `-Y` coloca-o em hibernação. `hdparm -S x` faz o disco rígido ser encerrado após um determinado período de inatividade. Substitua *x* como segue: `0` desabilita este mecanismo, fazendo com que o disco rígido seja executado continuamente. Valores de `1` a `240` são multiplicados por 5 segundos. Valores de `241` a `251` correspondem de 1 a 11 vezes 30 minutos.

As opções de economia de energia interna do disco rígido podem ser controladas pela opção `-B`. Selecione um valor de `0` a `255` para obter de economia máxima a throughput máximo. O resultado depende do disco rígido usado e é difícil de avaliar. Para tornar um disco rígido mais silencioso, use a opção `-M`. Selecione um valor de `128` a `254` para obter de silencioso à rápido.

Muitas vezes não é fácil colocar o disco rígido para hibernar. No Linux, vários processos gravam no disco rígido, ativando-o repetidamente. Portanto, é importante entender como o Linux trata os dados que necessitam ser gravados no disco rígido. Primeiro, todos os dados estão no buffer da memória RAM. O buffer é monitorado pelo daemon do kernel update (kupdated). Quando os dados atingem uma determinada idade limite ou quando o buffer está cheio até certo grau, o conteúdo do buffer é descarregado para o disco rígido. O tamanho do buffer é dinâmico e depende do tamanho da memória e da carga do sistema. Por padrão, kupdated é configurado em intervalos curtos para atingir a integridade de dados máxima. Verifica o buffer a cada 5 segundos e notifica o daemon do bdflush quando os dados têm mais de 30 segundos ou quando o buffer atinge um nível de preenchimento de 30%. Em seguida, o daemon do bdflush grava os dados no disco rígido. Também grava independentemente do kupdated se, por exemplo, o buffer estiver cheio.

ATENÇÃO: Deficiência da integridade de dados

Mudanças nas configurações do daemon de atualização do kernel colocam a integridade dos dados em perigo.

Além destes processos, sistemas de arquivo de registro em diário, como ReiserFS e Ext3, gravam seus metadados independentemente de bdflush, que também impede o disco rígido de ser encerrado. Para evitar isso, foi desenvolvida uma extensão especial

de kernel para dispositivos móveis. Consulte `/usr/src/linux/Documentation/laptop-mode.txt` para obter detalhes.

Outro fator importante é o modo como se comportam os programas ativos. Por exemplo, os bons editores gravam regularmente backups ocultos do arquivo modificado no momento para o disco rígido, fazendo com que ele saia do modo de hibernação. Recursos como este podem ser desabilitados às custas da integridade dos dados.

Com relação a isso, o mail daemon postfix faz uso da variável `POSTFIX_LAPTOP`. Se essa variável for configurada para `sim`, postfix acessa o disco rígido com muito menos freqüência. No entanto, isto é irrelevante se o intervalo pra kupdated for aumentado.

21.5 O Pacote powersave

O pacote `powersave` é responsável pela função de economia de energia em laptops durante a operação com bateria. Alguns dos seus recursos também são úteis para estações de trabalho e servidores normais, como suspender, standby, funcionalidade do botão ACPI e colocar os discos rígidos IDE para adormecer.

Este pacote contém todos os recursos de gerenciamento de energia do seu computador. Suporta hardware que usa discos rígidos ACPI, APM, IDE e tecnologias PowerNow! ou SpeedStep. As funcionalidades dos pacotes `apmd`, `acpid`, `ospmd` e `cpufreqd` (agora `cpuspeed`) foram consolidadas no pacote `powersave`. Daemons desses pacotes não devem ser executados simultaneamente com o daemon de economia de energia.

Mesmo que o seu sistema não contenha todos os elementos de hardware listados acima, use o daemon powersave para controlar a função de economia de energia. Como ACPI e APM excluem-se mutuamente, você só pode usar um destes sistemas no seu computador. O daemon detecta automaticamente quaisquer mudanças na configuração do hardware.

21.5.1 Configurando o Pacote powersave

Normalmente, a configuração de powersave é distribuída para vários arquivos:

/etc/sysconfig/powersave/common

Este arquivo contém configurações gerais para o daemon de economia de energia. Por exemplo, a quantidade de mensagens de depurar em `/var/log/messages` pode ficar maior, aumentando-se o valor da variável `DEBUG`.

/etc/sysconfig/powersave/events

O daemon de economia de energia precisa deste arquivo para processar eventos do sistema. Um evento pode receber atribuição de ações externas ou de ações realizadas pelo próprio daemon. Para as ações externas, o daemon tenta executar um arquivo executável em `/usr/lib/powersave/scripts/`. Ações internas predefinidas:

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby

`throttle` torna o processador mais lento de acordo com o valor definido em `MAX_THROTTLING`. Este valor depende do esquema atual. `dethrottle` configura o processador para desempenho total. `suspend_to_disk`, `suspend_to_ram` e `standby` acionam o evento do sistema para um modo adormecido. Essas três ações são de maneira geral responsáveis pelo acionamento do modo adormecido, mas elas devem ser sempre associadas a eventos específicos do sistema.

O diretório `/usr/lib/powersave/scripts` contém scripts para processamento de eventos:

notify

Notificação sobre um evento no console, na janela X ou sinal acústico.

screen_saver
Ativa a proteção de tela.

switch_vt
Útil se a tela for deslocada após suspensão ou standby.

wm_logout
Salva as configurações e efetua logout de GNOME, KDE ou outros gerenciadores de janela.

wm_shutdown
Salva as configurações GNOME ou KDE e desliga o sistema.

Se, por exemplo, a variável `EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"` for configurada, os dois scripts ou ações são processados na ordem especificada tão logo o usuário dê ao powersaved o comando para o modo adormecido `suspender para disco`. O daemon executa o script externo `/usr/lib/powersave/scripts/prepare_suspend_to_disk`. Após o script ser processado com êxito, o daemon executa a ação interna `do_suspend_to_disk` e configura o computador para o modo adormecido depois que o script tiver descarregado módulos críticos e interrompido serviços.

As ações para o evento de um botão adormecido podem ser modificadas como em `EVENT_BUTTON_SLEEP="notify suspend_to_disk"`. Neste caso, o usuário é informado sobre a suspensão pelo script externo `notify`. Em seguida, o evento `EVENT_GLOBAL_SUSPEND2DISK` é gerado, resultando na execução das ações mencionadas e um modo suspenso de sistema seguro. É possível personalizar o script `notify` com a variável `NOTIFY_METHOD` em `/etc/sysconfig/powersave/common`.

/etc/sysconfig/powersave/cpufreq
Contém variáveis para otimizar as configurações dinâmicas de freqüência da CPU.

/etc/sysconfig/powersave/battery
Contém limites de bateria e outras configurações específicas da bateria.

/etc/sysconfig/powersave/sleep
Neste arquivo, ative os modos adormecidos e determine que módulos críticos devem ser descarregados e que serviços devem ser interrompidos antes de um evento suspender ou aguardar. Quando o sistema é reiniciado, os módulos são recarregados

e os serviços iniciam novamente. Você pode até retardar um modo adormecido acionado, por exemplo, para gravar arquivos. As configurações padrões referem-se sobretudo aos módulos USB e PCMCIA. Normalmente, uma falha de suspender ou aguardar é causada por determinados módulos. Consulte Seção 21.5.4, “Solução de problemas” (p 295) para obter mais informações sobre identificação do erro.

/etc/sysconfig/powersave/cpufreq
Ativa o controle de resfriamento e térmico. Detalhes sobre este assunto estão disponíveis no arquivo `/usr/share/doc/packages/powersave/README.thermal`.

/etc/sysconfig/powersave/scheme_*
Estes são os vários esquemas que adaptam o consumo de energia a determinados cenários de distribuição. Vários esquemas são pré-configurados e podem ser usados na forma como são apresentados. Esquemas personalizados podem ser salvos aqui.

21.5.2 Configurando APM e ACPI

Suspender e Standby

Por padrão, os modos adormecidos são inativos, porque ainda não funcionam em alguns computadores. Há três modos adormecidos básicos de ACPI e dois de APM:

Suspender para Disco (ACPI S4, suspender APM)
Grava todo o conteúdo da memória no disco rígido. O computador é completamente desativado e não consome nenhuma energia.

Suspender para RAM (ACPI S3, suspender APM)
Grava os estados de todos os dispositivos na memória principal. Apenas a memória principal continua consumindo energia.

Standby (ACPI S1, APM standby)
Desativa alguns dispositivos (dependente do fabricante).

Verifique se as seguintes opções padrões estão configuradas no arquivo `/etc/sysconfig/powersave/events` para o correto processamento de suspender, standby e reiniciar (configurações padrões de acordo com a instalação do SUSE Linux):

```
EVENT_GLOBAL_SUSPEND2DISK=
"prepare_suspend_to_disk do_suspend_to_disk"
```

```
EVENT_GLOBAL_SUSPEND2RAM=
"prepare_suspend_to_ram do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
"prepare_standby do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
"restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
"restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
"restore_after_standby"
```

Estados de bateria padronizados

No arquivo `/etc/sysconfig/powersave/battery`, defina três níveis de carga de bateria (em porcentagem) que acionem alertas do sistema ou ações específicas quando forem atingidos.

```
BATTERY_WARNING=20
BATTERY_LOW=10
BATTERY_CRITICAL=5
```

As ações ou scripts a executar quando os níveis de carga caem abaixo dos limites especificados estão definidos no arquivo de configuração `/etc/sysconfig/powersave/events`. As ações padrões para botões podem ser modificadas como descrito em Seção 21.5.1, “Configurando o Pacote powersave” (p 289).

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Adaptando o consumo de energia a várias condições

O comportamento do sistema pode ser adaptado ao tipo de fonte de alimentação. O consumo de energia do sistema deve ser reduzido quando o sistema estiver desconectado da fonte de alimentação CA e operar com bateria. Da mesma maneira, o desempenho deve aumentar automaticamente, tão logo o sistema seja conectado à fonte de alimentação CA. A freqüência da CPU, a função de economia de energia de IDE e vários outros parâmetros podem ser modificados.

As ações a executar quando o computador for desconectado ou conectado à fonte de alimentação CA estão definidas em `/etc/sysconfig/powersave/events`. Selecione os esquemas a usar em `/etc/sysconfig/powersave/common`:

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

Os esquemas são armazenados em arquivos em `/etc/sysconfig/powersave`. Os nomes de arquivos têm o formato `scheme_name-of-the-scheme`. O exemplo refere-se a dois esquemas: `scheme_performance` e `scheme_powersave`. `desempenho`, `powersave`, `apresentaç o` e `acústico` são pré-configurados. Os esquemas existentes podem ser editados, criados, apagados ou associados com diferentes estados de fonte de alimentação com o auxílio do módulo gerenciamento de energia YaST descrito em Seção 21.6, “O módulo Gerenciamento de energia YaST” (p 297).

21.5.3 Recursos de ACPI adicionais

Se usar ACPI, você poderá controlar a resposta do seu sistema para os *botões ACPI* (energia, adormecido, tampa aberta e tampa fechada). Configure a execução das ações em `/etc/sysconfig/powersave/events`. Consulte este arquivo de configuração para obter uma explicação sobre as opções individuais.

EVENT_BUTTON_POWER="wm_shutdown"
Quando o botão de alimentação é pressionado, o sistema responde desligando o respectivo gerenciador de janela (KDE, GNOME, fvwm, etc.).

EVENT_BUTTON_SLEEP="suspend_to_disk"
Quando o botão adormecido é pressionado, o sistema é configurado para o modo suspend-to-disk.

EVENT_BUTTON_LID_OPEN="ignore"
Nada acontece quando a tampa está aberta.

EVENT_BUTTON_LID_CLOSED="screen_saver"
Quando a tampa está fechada, o protetor de tela é ativado.

É possível mais throttling do desempenho da CPU se a carga da CPU não exceder um limite especificado durante um período especificado. Especifique o limite de carga em `PROCESSOR_IDLE_LIMIT` e o tempo de espera em `CPU_IDLE_TIMEOUT`. Se a carga da CPU ficar abaixo do limite mais tempo do que o tempo de espera, o evento configurado em `EVENT_PROCESSOR_IDLE` é ativado. Se a CPU estiver ocupada novamente, `EVENT_PROCESSOR_BUSY` é executado.

21.5.4 Solução de problemas

Todas as mensagens de erro e alertas são registradas no arquivo `/var/log/messages`. Se não conseguir encontrar as informações necessárias, aumente o detalhamento das mensagens de economia de energia usando `DEBUG` no arquivo `/etc/sysconfig/powersave/common`. Aumente o valor da variável para `7` ou mesmo `15` e reinicie o daemon. As mensagens de erro mais detalhadas em `/var/log/messages` devem ajudá-lo a localizar o erro. As seguintes seções abordam os problemas mais comuns relacionados à economia de energia.

ACPI ativada com suporte de hardware mas funções não funcionam

Se você tiver problemas com a ACPI, use o comando `dmesg|grep -i acpi` para pesquisar a saída de `dmesg` para mensagens específicas à ACPI. Poderá ser necessário atualizar o BIOS para solucionar o problema. Na home page do fabricante do seu laptop, procure uma versão atualizada do BIOS e instale-a. Peça ao fabricante para estar em conformidade com a última especificação da ACPI. Se os erros persistirem após a atualização do BIOS, faça o seguinte para substituir a tabela DSDT defeituosa no seu BIOS com um DSDT atualizado:

1. Faça o download do DSDT para o seu sistema em `http://acpi.sourceforge.net/dsdt/tables`. Verifique se o arquivo está descompactado e compilado como mostra a extensão de arquivo `.aml` (linguagem computacional ACPI). Se for o caso, continue com a etapa 3.

2. Se a extensão de arquivo da tabela do download for `.asl` (linguagem fonte ACPI), compile-a com iasl (pacote `pmtools`). Digite o comando `iasl -sa file.asl`. A última versão de iasl (compilador ACPI da Intel) está disponível em `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.

3. Copie o arquivo `DSDT.aml` para qualquer localização (`/etc/DSDT.aml` é recomendada). Edite `/etc/sysconfig/kernel` e adapte o caminho para o arquivo DSDT de forma compatível. Inicie `mkinitrd` (pacote `mkinitrd`). Sempre que instalar o kernel e usar `mkinitrd` para criar um `initrd`, o DSDT modificado é integrado e carregado quando o sistema é inicializado.

A freqüência da CPU não funciona

Consulte as fontes de kernel (`kernel-source`) para ver se o seu processador é suportado. Você poderá precisar de um módulo de kernel ou de opção especial para ativar o controle de freqüência da CPU. Essas informações estão disponíveis em `/usr/src/linux/Documentation/cpu-freq/*`. Se for necessário um módulo especial ou de opção, configure-o no arquivo `/etc/sysconfig/powersave/cpufreq` por meio das variáveis `CPUFREQD_MODULE` e `CPUFREQD_MODULE_OPTS`.

Suspender e Standby não funcionam

Há vários problemas relacionados ao kernel que impedem o uso de suspender e standby nos sistemas da ACPI:

- Atualmente, os sistemas com mais de 1 GB de RAM não oferecem suporte a suspender.
- Atualmente, os sistemas multiprocessadores e sistemas com um processador P4 (com hyperthreading) não oferecem suporte a suspender.

O erro também pode ser devido à implementação errada de DSDT (BIOS). Se for o caso, instale um novo DSDT.

Em sistemas ACPI e APM: Quando o sistema tenta descarregar módulos defeituosos, o sistema é verificado ou o evento suspenso não é acionado. O mesmo também pode acontecer se você não descarregar módulos ou interromper serviços que impeçam suma suspensão bem-sucedida. Em ambos os casos, tente identificar o módulo defeituoso que impediu o modo adormecido. Os arquivos de registro gerados pelo daemon de economia de energia em `/var/log/sleep mode` são muito úteis em relação a isto. Se o computador não entrar no modo adormecido, a causa está no último módulo descarregado. Manipule as seguintes configurações em `/etc/sysconfig/powersave/sleep` para descarregar módulos problemáticos antes de suspender ou colocar em standby.

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

Se suspender ou colocar em standby ambientes de rede em transformação ou em conexão com sistemas de arquivo montados remotamente, como Samba e NIS, use automounter para montá-los ou adicionar os serviços respectivos como `smbfs` ou `nfs`, na variável acima mencionada. Se um aplicativo acessar o sistema de arquivo montado remotamente antes de suspender ou colocar em standby, o serviço não pode ser interrompido corretamente e o sistema de arquivo não pode ser desmontado de forma adequada. Após reiniciar o sistema, o sistema de arquivo pode estar corrompido e deve ser remontado.

Usando ACPI, a economia de energia não avisa os limites da bateria

Com ACPI, o sistema operacional pode solicitar ao BIOS para enviar uma mensagem quando o nível de carga da bateria cair abaixo de determinado limite. A vantagem deste método é que o estado da bateria não precisa ser pesquisado constantemente, o que prejudicaria o desempenho do computador. Contudo, esta notificação pode não ocorrer quando o nível de carga cai baixo do limite especificado, mesmo que, supostamente, o BIOS suporte este recurso. Se isto acontecer no seu sistema, configure a variável `FORCE_BATTERY_POLLING` no arquivo `/etc/sysconfig/powersave/battery` em `sim` para forçar o polling da bateria.

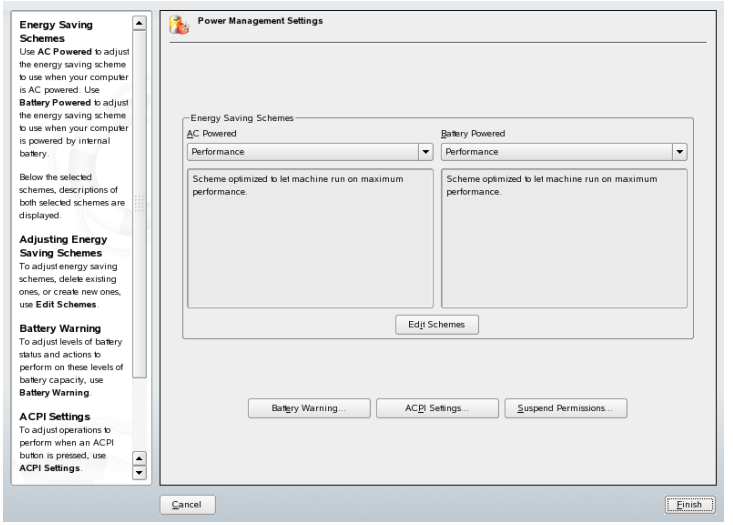
21.5.5 Para obter mais informações

Informações sobre o pacote powersave também estão disponíveis em `/usr/share/doc/packages/powersave`.

21.6 O módulo Gerenciamento de energia YaST

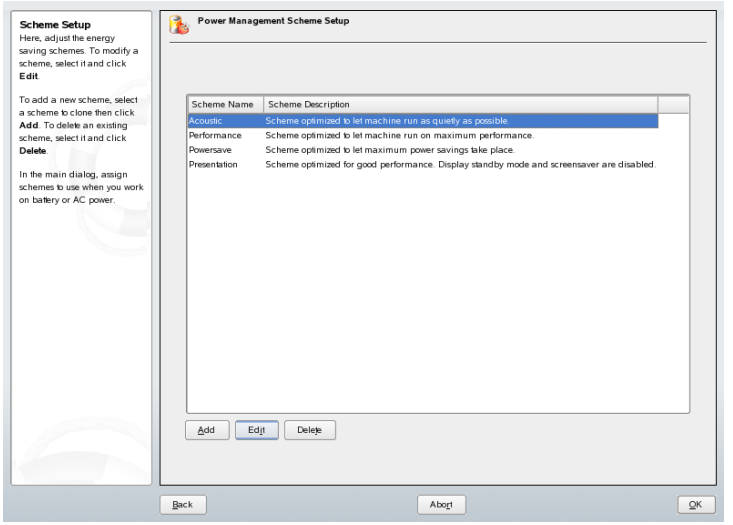
O módulo de gerenciamento de energia YaST pode definir todas as configurações de gerenciamento de energia já descritas. Quando iniciado no Centro de Controle YaST com *Sistema → Gerenciamento de Energia*, a primeira caixa de diálogo se abre. Isso é mostrado em Figura 21.1, “Seleção de Esquema” (p 298).

Figura 21.1 *Seleção de Esquema*


Energy Saving Schemes
Use AC Powered to adjust the energy saving scheme to use when your computer is AC powered. Use Battery Powered to adjust the energy saving scheme to use when your computer is powered by internal battery.
Below the selected schemes, descriptions of both selected schemes are displayed.
Adjusting Energy Saving Schemes
To adjust energy saving schemes, delete existing ones, or create new ones, use Edit Schemes.
Battery Warning
To adjust levels of battery status and actions to perform on these levels of battery capacity, use Battery Warning.
ACPI Settings
To adjust operations to perform when an ACPI button is pressed, use ACPI Settings.
Power Management Settings
Energy Saving Schemes
AC Powered
Performance
Scheme optimized to let machine run on maximum performance.
Battery Powered
Performance
Scheme optimized to let machine run on maximum performance.
Edit Schemes
Battery Warning...
ACPI Settings...
Suspend Permissions...
Cancel
Finish

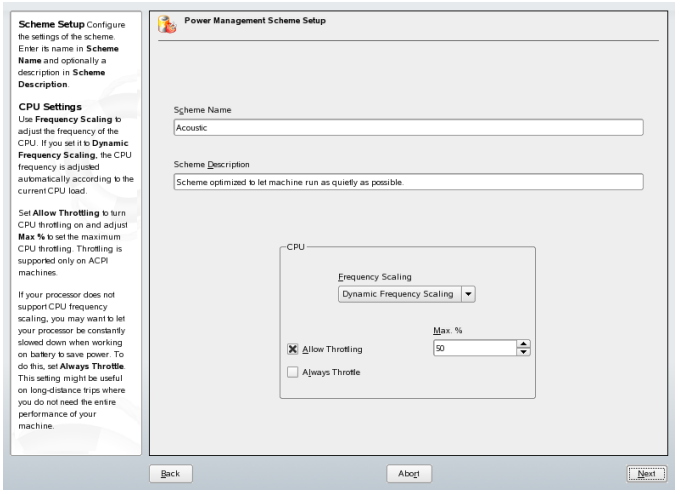
Nesta caixa de diálogo, selecione os esquemas a usar na operação a bateria e na operação de CA. Para adicionar ou modificar os esquemas, clique em *Editar Esquemas*, que abre uma visão geral dos esquemas existentes como a da Figura 21.2, “Visão geral dos esquemas existentes” (p 299).

Figura 21.2 *Visão geral dos esquemas existentes*


Scheme Setup
Here, adjust the energy saving schemes. To modify a scheme, select it and click Edit.
To add a new scheme, select a scheme to clone then click Add. To delete an existing scheme, select it and click Delete.
In the main dialog, assign schemes to use when you work on battery or AC power.
Power Management Scheme Setup
Scheme Name
Scheme Description
Acoustic
Scheme optimized to let machine run as quietly as possible.
Performance
Scheme optimized to let machine run on maximum performance.
Powersave
Scheme optimized to let maximum power savings take place.
Presentation
Scheme optimized for good performance. Display standby mode and screensaver are disabled.
Add
Edit
Delete
Back
Abort
OK

Na visão geral dos esquemas, selecione o esquema a modificar e clique em *Editar*. Para criar um novo esquema, clique em *Adicionar*. A caixa de diálogo que abre é a mesma nos dois casos e é mostrada em Figura 21.3, “Configurando um esquema” (p 299).

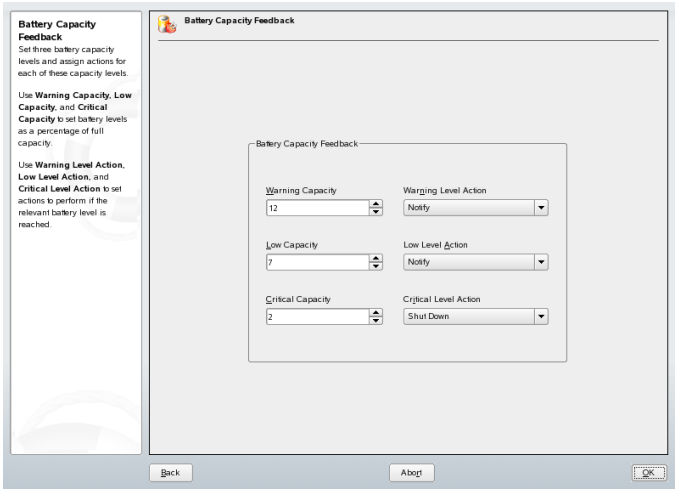
Figura 21.3 *Configurando um esquema*


Scheme Setup Configure the settings of the scheme. Enter its name in Scheme Name and optionally a description in Scheme Description.
CPU Settings
Use Frequency Scaling to adjust the frequency of the CPU. If you set it to Dynamic Frequency Scaling, the CPU frequency is adjusted automatically according to the current CPU load.
Set Allow Throttling to turn CPU throttling on and adjust Max % to set the maximum CPU throttling. Throttling is supported only on ACPI machines.
If your processor does not support CPU frequency scaling, you may want to let your processor be constantly slowed down when working on battery to save power. To do this, set Always Throttle. This setting might be useful on long-distance trips where you do not need the entire performance of your machine.
Power Management Scheme Setup
Scheme Name
Acoustic
Scheme Description
Scheme optimized to let machine run as quietly as possible.
CPU
Frequency Scaling
Dynamic Frequency Scaling
Max. %
50
Allow Throttling
Always Throttle
Back
Abort
Next

Primeiro, digite um nome adequado e uma descrição para o esquema novo ou editado. Determine se e como o desempenho da CPU deve ser controlado para este esquema. Decida se e em que medida o dimensionamento de freqüência e o throttling devem ser usados. Na caixa de diálogo seguinte para o disco rígido, defina uma *Política de Standby* para desempenho máximo ou para economia de energia. A *Política de Acústica* controla o nível de ruído do disco rígido (suportado por poucos discos rígidos). A *Política de Resfriamento* determina o método de resfriamento a ser usado. Infelizmente, este tipo de controle térmico raras vezes é suportado pelo BIOS. Leia `/usr/share/doc/packages/powersave/README.thermal` para aprender como usar o ventilador e métodos de resfriamento passivos.

As configurações globais de gerenciamento de energia também podem ser feitas da caixa de diálogo inicial usando *Alerta de Bateria*, *Configurações ACPI* ou *Habilitar Suspend*. Clique em *Alerta de Bateria* para acessar a caixa de diálogo do nível de carga de bateria, mostrada em Figura 21.4, “Nível de carga de bateria” (p 300).

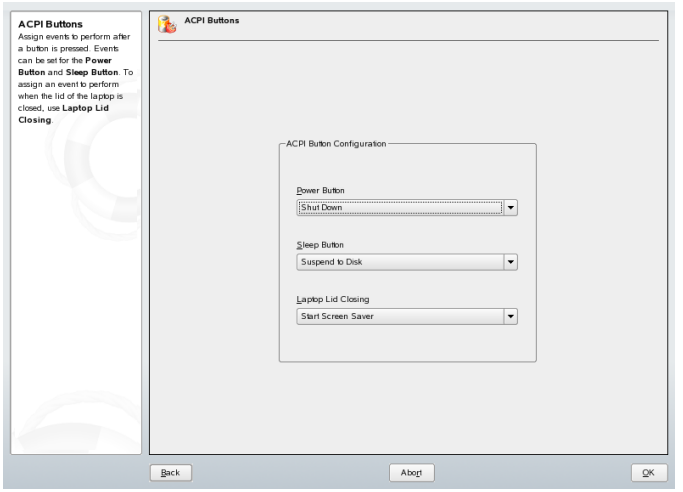
Figura 21.4 *Nível de carga de bateria*


Battery Capacity Feedback
Set three battery capacity levels and assign actions for each of these capacity levels.
Use Warning Capacity, Low Capacity, and Critical Capacity to set battery levels as a percentage of full capacity.
Use Warning Level Action, Low Level Action, and Critical Level Action to set actions to perform if the relevant battery level is reached.
Battery Capacity Feedback
Battery Capacity Feedback
Warning Capacity
12
Warning Level Action
Notify
Low Capacity
7
Low Level Action
Notify
Critical Capacity
2
Critical Level Action
Shut Down
Back
Abort
OK

O BIOS do seu sistema notifica o sistema operacional sempre que o nível de carga cai abaixo de certos limites configuráveis. Nesta caixa de diálogo, defina três limites: *Alerta de Capacidade*, *Capacidade Baixa* e *Capacidade Crítica*. Ações específicas são acionadas quando o nível de carga cai abaixo desses limites. Normalmente, os dois primeiros estados apenas acionam uma notificação para o usuário. O terceiro nível crítico aciona um shutdown, porque a energia restante não é suficiente para operação

continuada do sistema. Selecione os níveis de carga adequados e as ações desejadas e clique em *OK* para retornar à caixa de diálogo de inicialização.

Figura 21.5 *Configurações ACPI*


ACPI Buttons
Assign events to perform after a button is pressed. Events can be set for the Power Button and Sleep Button. To assign an event to perform when the lid of the laptop is closed, use Laptop Lid Closing.
ACPI Buttons
ACPI Button Configuration
Power Button
Shut Down
Sleep Button
Suspend to Disk
Laptop Lid Closing
Start Screen Saver
Back
Abort
OK

Acesse a caixa de diálogo para configurar os botões de ACPI usando *Configurações ACPI*. Isso é mostrado em Figura 21.5, “Configurações ACPI” (p 301). As configurações dos botões de ACPI determinam como o sistema deve responder a certos switches. Configure a resposta do sistema ao pressionar o botão de energia e o botão sleep e ao fechar a tampa do laptop. Clique em *OK* para concluir a configuração e retornar à caixa de diálogo inicial.

Clique em *Habilitar Suspensão* para inserir uma caixa de diálogo na qual determinar se e como os usuários deste sistema podem usar a funcionalidade suspender ou aguardar. Clique em *OK* para retornar à caixa de diálogo principal. Clique em *OK* novamente para sair do módulo e confirmar as suas configurações de gerenciamento de energia.

22 Comunicação sem fio

Há várias possibilidades de usar o sistema Linux para estabelecer comunicação com outros computadores, telefones celulares ou dispositivos periféricos. A WLAN (wireless LAN - LAN sem fio) pode ser usada para colocar laptops em rede. O bluetooth pode ser usado para conectar componentes individuais do sistema (mouse, teclado), dispositivos periféricos, telefones celulares, PDAs e computadores individuais uns com os outros. O IrDA é mais usado para comunicação com PDAs ou telefones celulares. Este capítulo introduz todas as três tecnologias e sua configuração.

22.1 LAN sem fio

As LANs sem fio tornaram-se um aspecto indispensável da computação móvel. Atualmente, a maioria dos laptops tem placas WLAN embutidas. O padrão 802.11 para a comunicação sem fio de placas WLAN foi preparado pela organização IEEE. Originalmente, este padrão forneceu uma taxa de transmissão máxima de 2 MBit/s. Entretanto, vários suplementos foram adicionados para aumentar a taxa de dados. Esses suplementos definem detalhes como a modulação, saída de transmissão e taxas de transmissão:

Tabela 22.1 *Visão geral de vários padrões WLAN*

Nome	Banda (GHz)	Taxa de transmissão máxima (MBit/s)	Nota
802.11	2.4	2	Desatualizado; praticamente nenhum dispositivo final disponível
802.11b	2.4	11	Comum
802.11a	5	54	Menos comum
802.11g	2.4	54	Compatibilidade retroativa com 11b

Além disso, existem padrões patenteados, como a variação 802.11b da Texas Instruments com uma taxa de transmissão máxima de 22 MBit/s (às vezes conhecida como 802.11b+). Porém, a popularidade de placas que utilizam este padrão é limitada.

22.1.1 Hardware

Placas 802.11 não são suportadas pelo SUSE Linux. A maioria das placas que utilizam 802.11a, 802.11b e 802.11g é suportada. Placas novas normalmente são compatíveis com o padrão 802.11g, mas as placas que utilizam o 802.11b ainda estão disponíveis. Normalmente, placas com os seguintes chips são suportadas:

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT

- Lucent/Agere Hermes
- Ralink RT2400, RT2500
- Texas Instruments ACX100, ACX111
- ZyDAS zd1201

Várias placas antigas que raramente são usadas e que não estão mais disponíveis também são suportadas. Uma ampla lista de placas WLAN e os chips que elas utilizam está disponível no site da Web da *AbsoluteValue Systems* no endereço http://www.linux-wlan.org/docs/wlan_adapters.html.gz. http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz oferece uma visão geral de vários chips WLAN.

Algumas placas precisam de uma imagem de firmware que deve ser carregada na placa quando o driver é inicializado. Isto acontece com o Intersil PrismGT, Atmel e TI ACX100 e ACX111. O firmware pode ser facilmente instalado com a Atualização Online YaST. O firmware para placas Intel PRO/Wireless é fornecido com o SUSE Linux e é instalado automaticamente pelo YaST assim que uma placa desse tipo é detectada. Mais informações sobre esse assunto estão disponíveis no sistema instalado em `/usr/share/doc/packages/wireless-tools/README.firmware`.

Placas sem o suporte nativo do Linux podem ser usadas com a execução do aplicativo ndiswrapper. O ndiswrapper utiliza os drivers do Windows que são fornecidos junto com a maioria das placas WLAN. É possível encontrar uma descrição do ndiswrapper em `/usr/share/doc/packages/ndiswrapper/README.SUSE` quando o pacote `ndiswrapper` é instalado. Para obter informações mais detalhadas sobre ndiswrapper, consulte o site da Web do projeto em http://ndiswrapper.sourceforge.net/support.html.

22.1.2 Função

Nas redes sem fio, várias técnicas e configurações são usadas para assegurar conexões rápidas, seguras e com alta qualidade. Tipos operacionais diferentes adaptam-se a configurações diferentes. Pode ser difícil escolher o método de autenticação correto. Os métodos de criptografia disponíveis possuem diferentes vantagens e armadilhas.

Modo de funcionamento

Basicamente, as redes sem fio podem ser classificadas como redes gerenciadas e redes ad-hoc. As redes gerenciadas possuem um elemento de gerenciamento: o ponto de acesso. Neste modo (também conhecido como modo de infra-estrutura), todas as conexões das estações WLAN na rede passam pelo ponto de acesso, que também pode servir como uma conexão para uma ethernet. Redes ad-hoc não possuem um ponto de acesso. As estações se comunicam diretamente umas com as outras. A faixa de transmissão e o número de estações participantes são muito limitados nas redes ad-hoc. Portanto, um ponto de acesso normalmente é mais eficiente. É até mesmo possível usar uma placa WLAN como um ponto de acesso. A maioria das placas suporta esta funcionalidade.

Como uma rede sem fio é muito mais fácil de interceptar e comprometer do que uma rede com fio, os vários padrões incluem métodos de autenticação e criptografia. Na versão original do padrão IEEE 802.11, esses métodos são descritos sob o termo WEP. Porém, como foi provado que o WEP não é seguro (consulte a "Segurança" (p 312)), a indústria WLAN (reunida sob o nome *Wi-Fi Alliance*) definiu uma nova extensão, chamada WPA, que supostamente elimina os pontos fracos do WEP. O padrão IEEE 802.11i posterior (também conhecido como WPA2, porque o WPA é baseado em uma versão de rascunho do 802.11i) inclui o WPA e alguns outros métodos de autenticação e criptografia.

Autenticação

Para garantir que apenas as estações autorizadas possam se conectar, vários mecanismos de autenticação são usados em redes gerenciadas:

Aberto
: Um sistema aberto é um sistema que não precisa de autenticação. Qualquer estação pode se juntar à rede. Contudo, a criptografia WEP (consulte a "Criptografia" (p 308)) pode ser usada.

Chave compartilhada (de acordo com o padrão IEEE 802.11)
: Neste procedimento, a chave WEP é usada para autenticação. Porém, este procedimento não é recomendado, porque torna a chave WEP mais suscetível a ataques. Tudo o que um invasor precisa fazer é escutar durante tempo suficiente a comunicação entre a estação e o ponto de acesso. Durante o processo de autenticação, ambos os lados trocam as mesmas informações, uma vez de forma criptografada e

outra de forma não criptografada. Isso possibilita a reconstrução da chave com as ferramentas adequadas. Como esse método utiliza a chave WEP para a autenticação e para a criptografia, ele não melhora a segurança da rede. Uma estação com a chave WEP correta pode ser autenticada, criptografada e descriptografada. Uma estação que não tem a chave não pode descriptografar os pacotes recebidos. Da mesma maneira, ela não pode se comunicar, mesmo que tenha que se autenticar.

WPA-PSK (de acordo com o padrão IEEE 802.1x)

O WPA-PSK (PSK corresponde a preshared key - chave pré-compartilhada) funciona de maneira semelhante ao procedimento Chave compartilhada. Todas as estações participantes, assim como o ponto de acesso, precisam da mesma chave. A chave tem 256 bits de tamanho e normalmente é digitada como uma frase secreta. Este sistema não precisa de um gerenciamento de chave complexo como o WPA-EAP e é mais adequado para uso privado. Portanto, o WPA-PSK é às vezes conhecido como WPA "Home".

WPA-EAP (de acordo com o padrão IEEE 802.1x)

Na verdade, o WPA-EAP não é um sistema de autenticação, e sim um protocolo para transporte de informações de autenticação. O WPA-EAP é usado para proteger redes sem fio em empresas. Em redes privadas, ele é raramente usado. Por este motivo, o WPA-EAP é às vezes conhecido como WPA "Enterprise".

O WPA-EAP precisa de um servidor Radius para autenticar os usuários. O EAP oferece três métodos diferentes de conexão e autenticação no servidor: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) e PEAP (Protected Extensible Authentication Protocol). Em resumo, essas opções funcionam da seguinte maneira:

EAP-TLS

A autenticação TLS utiliza a troca mútua de certificados para servidor e cliente. Primeiro, o servidor apresenta o seu certificado para o cliente, onde ele é avaliado. Se o certificado for considerado válido, o cliente, por sua vez, apresenta o seu certificado para o servidor. Embora o TLS seja seguro, ele exige uma infra-estrutura de gerenciamento de certificação que funcione em sua rede. Esta infra-estrutura é raramente encontrada em redes particulares.

EAP-TTLS e PEAP

Os protocolos TTLS e PEAP são protocolos de dois estágios. No primeiro estágio, a segurança é estabelecida e, no segundo, os dados de autenticação do

cliente são trocados. Eles exigem muito menos overhead de gerenciamento de certificação do que o TLS, se houver.

Criptografia

Existem vários métodos de criptografia para assegurar que pessoas não autorizadas não possam ler os pacotes de dados que são trocados em uma rede sem fio nem obter acesso à rede:

WEP (definido no padrão IEEE 802.11)
Este padrão utiliza o algoritmo de criptografia RC4, originalmente com um tamanho de chave de 40 bits, posteriormente também com 104 bits. Muitas vezes, o tamanho é declarado como 64 bits ou 128 bits, dependendo da inclusão ou não dos 24 bits do vetor de inicialização. Porém, este padrão possui algumas fraquezas. Os ataques contra as chaves geradas por este sistema podem ser bem-sucedidos. Contudo, é melhor usar o WEP do que não criptografar a rede de nenhuma maneira.

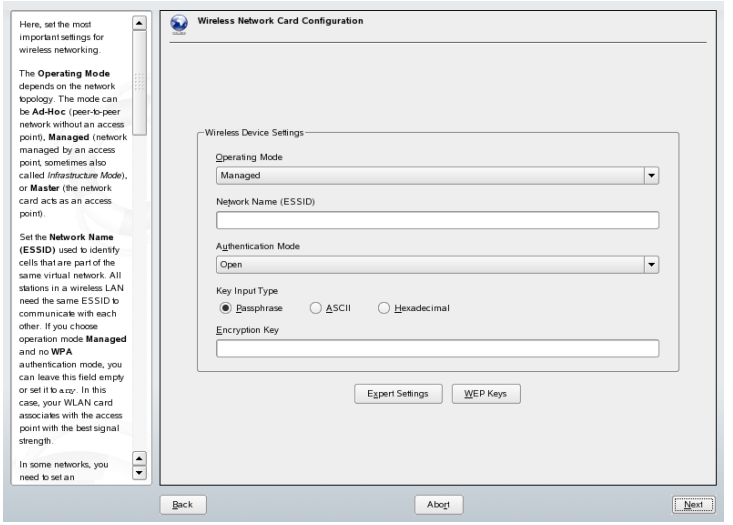
TKIP (definido no padrão WPA/IEEE 802.11i)
Este protocolo de gerenciamento de chave definido no padrão WPA utiliza o mesmo algoritmo de criptografia do WEP, mas elimina sua fraqueza. Como uma nova chave é gerada para cada pacote de dados, os ataques contra essas chaves são em vão. O TKIP é usado junto com o WPA-PSK.

CCMP (definido no padrão IEEE 802.11i)
O CCMP descreve o gerenciamento de chave. Normalmente, ele é usado na conexão com o WPA-EAP, mas também pode ser usado com o WPA-PSK. A criptografia acontece de acordo com o AES e é mais forte do que a criptografia RC4 do padrão WEP.

22.1.3 Configuração com YaST

Para configurar uma placa de rede sem fio, inicio o módulo *Placa de Rede* do YaST. Em *Configuração de Endereço de Rede*, selecione o tipo de dispositivo *Sem Fio* e clique em *Próximo*. Em *Configuração de Placa de Rede Sem Fio*, exibido na Figura 22.1, “YaST Configurando a placa de rede sem fio” (p 309), defina as configurações básicas para a operação da WLAN:

Figura 22.1 *YaST Configurando a placa de rede sem fio*


Here, set the most important settings for wireless networking.
The Operating Mode depends on the network topology. The mode can be Ad-Hoc (peer-to-peer network without an access point), Managed (network managed by an access point, sometimes also called Infrastructure Mode), or Master (the network card acts as an access point).
Set the Network Name (ESSID) used to identify cells that are part of the same virtual network. All stations in a wireless LAN need the same ESSID to communicate with each other. If you choose operation mode Managed and no WPA authentication mode, you can leave this field empty or set it to any. In this case, your WLAN card associates with the access point with the best signal strength.
In some networks, you need to set an
Wireless Network Card Configuration
Wireless Device Settings
Operating Mode
Managed
Network Name (ESSID)
Authentication Mode
Open
Key Input Type
Passphrase
ASCII
Hexadecimal
Encryption Key
Expert Settings
WEP Keys
Back
Abort
Next

Modo de funcionamento

Uma estação pode ser integrada em uma WLAN de três modos diferentes. O modo mais adequado depende da rede na qual deve ocorrer a comunicação: *Ad-hoc* (rede não-hierárquica sem ponto de acesso), *Gerenciada* (a rede é gerenciada por um ponto de acesso) ou *Master* (sua placa de rede deve ser usada como o ponto de acesso). Para usar qualquer um dos modos WPA-PSK ou WPA-EAP, o modo de funcionamento deverá ser definido como *gerenciado*.

Nome da Rede (ESSID)

Todas as estações em uma rede sem fio precisam do mesmo ESSID para se comunicar umas com as outras. Se nenhuma opção for especificada, a placa selecionará automaticamente um ponto de acesso, que pode não ser o desejado.

Modo de Autenticação

Selecione um método de autenticação adequado para a sua rede: *Abra*, *Chave Compartilhada*, *WPA-PSK* ou *WPA-EAP*. Se você selecionar a autenticação WPA, um nome de rede deverá ser definido.

Configurações de Usuário Avançado

Este botão abre uma caixa de diálogo com as configurações detalhadas da sua conexão WLAN. Uma descrição detalhada desta caixa de diálogo será fornecida posteriormente.

Após serem completadas as configurações básicas, a sua estação estará pronta para a distribuição na WLAN.

IMPORTANTE: Segurança em redes sem fio

Certifique-se de usar um dos métodos de autenticação e criptografia suportados para proteger o tráfego da rede. As conexões de WLAN não criptografadas permitem que terceiros interceptem todos os dados da rede. Mesmo uma criptografia mais fraca (WEP) é melhor do que nenhuma. Consulte a "Criptografia" (p 308) e a "Segurança" (p 312) para obter mais informações.

Dependendo do método de autenticação selecionado, o YaST solicita que você faça um ajuste fino das configurações em outra caixa de diálogo. Para a opção *Aberto*, não há nada para definir, porque essa configuração implementa operações não criptografadas sem autenticação.

Chaves WEP

Defina um tipo de entrada de chave. Selecione dentre *Frase Secreta*, *ASCII* ou *Hexadecimal*. É possível manter até quatro chaves diferentes para criptografar os dados transmitidos. Clique em *Várias Chaves* para informar a caixa de diálogo de configuração de chave. Defina o tamanho da chave: *128 bits* ou *64 bits*. A configuração padrão é *128 bits*. Na área de listas na parte inferior da caixa de diálogo, até quatro chaves diferentes podem ser especificadas para serem usadas pela sua estação para a criptografia. Pressione *Definir como Padrão* para definir uma delas como a chave padrão. A não ser que você mude a opção, o YaST utiliza a primeira chave informada como a chave padrão. Se a chave padrão for apagada, uma das outras chaves deverá ser marcada manualmente como a chave padrão. Clique em *Editar* para modificar as entradas de lista existentes ou criar novas chaves. Neste caso, uma janela pop-up solicita que você selecione um tipo de entrada (*Frase Secreta*, *ASCII* ou *Hexadecimal*). Se você selecionar *Frase Secreta*, digite uma palavra ou string de caractere da qual uma chave é gerada de acordo com o tamanho especificado anteriormente. O *ASCII* exige uma entrada de 5 caracteres para uma chave de 64 bits e 13 caracteres para uma chave de 128 bits. Para a opção *Hexadecimal*, digite 10 caracteres para uma chave de 64 bits ou 26 caracteres para uma chave de 128 bits em notação hexadecimal.

WPA-PSK

Para digitar uma chave para WPA-PSK, selecione o método de entrada *Frase Secreta* ou *Hexadecimal*. No modo *Frase Secreta*, a entrada deve ser de 8 a 63 caracteres. No modo *Hexadecimal*, digite 64 caracteres.

WPA-EAP

Digite as credenciais fornecidas pelo seu administrador de rede. Para TLS, forneça o *Certificado de Cliente* e o *Certificado de Servidor*. TTLS e PEAP exigem *Identidade* e *Senha*. O *Certificado de Servidor* é opcional. O YaST procura algum certificado em `/etc/cert`, então grave os certificados dados a você neste local e restrinja o acesso a esses arquivos a `0600` (leitura e gravação do proprietário).

Clique em *Configurações de Usuário Avançado* para sair da caixa de diálogo para a configuração básica da conexão WLAN e informe a configuração de usuário avançado. As seguintes opções estão disponíveis nesta caixa de diálogo:

Canal

A especificação de um canal no qual a estação WLAN deve funcionar é necessária somente nos modos *Ad-hoc* e *Master*. No modo *Gerenciado*, a placa pesquisa automaticamente os canais disponíveis para pontos de acesso. No modo *Ad-hoc*, selecione um dos 12 canais oferecidos para a comunicação da sua estação com as outras estações. No modo *Master*, determine em qual canal a sua placa deve oferecer funcionalidade de ponto de acesso. A configuração padrão para esta opção é *Auto*.

Taxa de Bits

Dependendo do desempenho da sua rede, você pode definir uma determinada taxa de bits para a transmissão de um ponto para outro. Na configuração padrão *Automático*, o sistema tenta usar a taxa de transmissão de dados mais alta possível. Algumas placas WLAN não suportam a configuração da taxa de bits.

Ponto de Acesso

Em um ambiente com vários pontos de acesso, um deles pode ser pré-selecionado especificando-se o endereço MAC.

Utilizar o Gerenciamento de Energia

Quando você estiver em trânsito, use as tecnologias de gerenciamento de energia para maximizar o tempo de funcionamento da bateria. Mais informações sobre o gerenciamento de energia estão disponíveis no Capítulo 21, *Gerenciamento de energia* (p 277).

22.1.4 Utilitários

O hostap (pacote `hostap`) é usado para executar uma placa WLAN como um ponto de acesso. Mais informações sobre este pacote estão disponíveis na home page do projeto (`http://hostap.epitest.fi/`).

O kismet (pacote `kismet`) é uma ferramenta de diagnóstico de rede com a qual é possível escutar o tráfego de pacote WLAN. Desta forma, você também pode detectar quaisquer tentativas de invasão na rede. Mais informações estão disponíveis em `http://www.kismetwireless.net/` e na página do manual.

22.1.5 Dicas sobre a configuração de uma WLAN

Essas dicas podem ajudar a ajustar a velocidade e a estabilidade, assim como os aspectos de segurança da sua WLAN.

Estabilidade e velocidade

O desempenho e a confiabilidade de uma rede sem fio dependem principalmente do fato de as estações participantes receberem ou não um sinal claro das outras estações. Obstruções como paredes podem enfraquecer grandemente o sinal. Quanto menor a força do sinal, mais lenta fica a transmissão. Durante a operação, verifique a força do sinal com o utilitário iwconfig na linha de comando (campo `Qualidade do Link`) ou com o KInternet no KDE. Se tiver problemas com a qualidade do sinal, tente configurar os dispositivos em outro lugar ou ajuste a posição das antenas do seu ponto de acesso. Antenas auxiliares que melhoram substancialmente a recepção estão disponíveis para várias placas PCMCIA WLAN. A taxa especificada pelo fabricante, como 54 MBit/s, é um valor nominal que representa o máximo teórico. Na prática, o throughput máximo de dados não passa da metade desse valor.

Segurança

Se você desejar configurar uma rede sem fio, lembre-se de que qualquer pessoa dentro da faixa de transmissão poderá acessá-la facilmente se não forem implementadas medidas de segurança. Portanto, certifique-se de ativar o método de criptografia. Todas as placas

WLAN e pontos de acesso suportam a criptografia WEP. Embora ainda não seja completamente segura, ela representa um obstáculo para um invasor em potencial. A criptografia WEP é normalmente adequada para uso particular. A WPA-PSK é ainda melhor, mas não é implementada em pontos de acesso ou roteadores antigos com funcionalidade WLAN. Em alguns dispositivos, o WPA pode ser implementado por meio de uma atualização de firmware. Além disso, o Linux não suporta o WPA em todos os componentes de hardware. Quando esta documentação estava sendo preparada, o WPA funcionava somente com placas que utilizavam chips Atheros, Intel PRO/Wireless ou Prism2/2.5/3. No chip Prism2/2.5/3, o WPA funcionava somente se o driver hostap estivesse em uso (consulte a “Problemas com placas Prism2” (p 313)). Se o WPA não estiver disponível, é melhor utilizar a criptografia WEP do que nenhum tipo de criptografia. Em empresas com requisitos de segurança avançados, as redes sem fio devem ser operadas somente com WPA.

22.1.6 Solução de problemas

Se a sua placa WLAN falhar na resposta, verifique se realizou o download do firmware necessário. Consulte a Seção 22.1.1, “Hardware” (p 304). Os parágrafos a seguir descrevem alguns problemas conhecidos.

Vários dispositivos de rede

Os laptops modernos normalmente possuem uma placa de rede e uma placa WLAN. Se você configurou ambos os dispositivos com DHCP (designação automática de endereço), poderá encontrar problemas com a resolução de nome e o gateway padrão. Isto fica evidente quando você pode efetuar ping no roteador, mas não pode navegar na Internet. O Banco de Dados de Suporte no endereço `http://portal.suse.com` apresenta um artigo sobre o assunto. Para encontrar o artigo, digite “DHCP” na caixa de diálogo de pesquisa.

Problemas com placas Prism2

Vários drivers estão disponíveis para dispositivos com chips Prism2. As várias placas funcionam mais ou menos adequadamente com os vários drivers. Com essas placas, a criptografia WPA somente pode ser usada com o driver hostap. Se tal placa não funcionar adequadamente ou não funcionar ou se você desejar usar a criptografia WPA, leia `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

O suporte a criptografia WPA é muito novo no SUSE Linux e ainda está em desenvolvimento. Além disso, o YaST não suporta a configuração de todos os métodos de autenticação WPA. Nem todas as placas e drivers LAN suportam a criptografia WPA. Algumas placas precisam de uma atualização do firmware para habilitar a criptografia WPA. Se você deseja usar a criptografia WPA, leia `/usr/share/doc/packages/wireless-tools/README.wpa`.

22.1.7 Mais informações

As páginas da Internet de Jean Tourrilhes, que desenvolveu as *Ferramentas Sem Fio* para o Linux, apresentam uma grande variedade de informações sobre dispositivos sem fio. Consulte a página `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`.

22.2 Bluetooth

Bluetooth é uma tecnologia sem fio para conexão de vários dispositivos, como telefones celulares, PDAs, dispositivos periféricos ou componentes de sistema como teclado ou mouse. O nome deriva do rei dinamarquês Harold Bluetooth, que uniu várias facções guerreiras na Escandinávia. O logotipo da Bluetooth baseia-se nas runas de “H” (lembra uma estrela) e “B”.

Vários aspectos importantes distinguem o Bluetooth do IrDA. Primeiro, os dispositivos individuais não precisam “ver” um ao outro diretamente e, segundo, vários dispositivos podem ser conectados em uma rede. Contudo, a taxa de dados máxima é de 720 Kbps (na versão atual 1.2). Teoricamente, o Bluetooth pode se comunicar até através de paredes. Na prática, porém, isto depende das propriedades da parede e da classe do dispositivo. Há três classes de dispositivos com faixas de transmissão entre dez e 100 metros.

22.2.1 Noções básicas

As seções a seguir resumem os princípios básicos da maneira como o Bluetooth trabalha. Obtenha mais informações sobre os requisitos que o software deve atender, como o Bluetooth interage com o seu sistema e como ele traça o seu perfil de trabalho.

Software

Para poder usar o Bluetooth, você precisa de um adaptador de Bluetooth (adaptador interno ou dispositivo externo), drivers e uma pilha de protocolos Bluetooth. O kernel do Linux já contém os drivers básicos para usar o Bluetooth. O sistema Bluez é usado como pilha de protocolos. Para verificar se os aplicativos funcionam com o Bluetooth, os pacotes básicos `bluez-libs` e `bluez-utils` devem estar instalados. Esses pacotes oferecem diversos serviços e utilitários necessários. Além disso, alguns adaptadores, como Broadcom ou AVM BlueFritz! exigem que o pacote `bluez-firmware` seja instalado. O pacote `bluez-cups` habilita a impressão nas conexões Bluetooth.

Interação geral

Um sistema Bluetooth consiste em quatro camadas interbloqueadas que fornecem a funcionalidade desejada:

Hardware
: O adaptador e um driver adequado para suporte pelo kernel do Linux.

Arquivos de configuração
: Usados para controlar o sistema Bluetooth.

Daemons
: Serviços que são controlados pelos arquivos de configuração e fornecem a funcionalidade.

Aplicativos
: Os aplicativos possibilitam que a funcionalidade fornecida pelos daemons seja usada e controlada pelo usuário.

Ao inserir um adaptador Bluetooth, seu driver é carregado pelo sistema hotplug. Depois que o driver for carregado, o sistema verifica os arquivos de configuração para ver se

o Bluetooth deve ser iniciado. Se for o caso, determina os serviços a serem iniciados. Com base nestas informações, os daemons respectivos são iniciados. Os adaptadores Bluetooth são examinados durante a instalação. Se for encontrado um ou mais, o Bluetooth é habilitado. Caso contrário, o sistema Bluetooth é desativado. Qualquer dispositivo Bluetooth acrescentado depois deve ser habilitado manualmente.

Perfis

No Bluetooth, os serviços são definidos por meio de perfis, como o perfil de transferência de arquivo, o perfil de impressão básica e o perfil de rede de área pessoal. Para habilitar um dispositivo para usar os serviços de outro dispositivo, ambos devem compreender o mesmo perfil. Freqüentemente, essa parte das informações não é incluída no pacote e no manual do dispositivo. Infelizmente, alguns fabricantes não atendem rigorosamente as definições dos perfis individuais. Apesar disto, a comunicação entre os dispositivos em geral funciona uniformemente.

No texto a seguir, os dispositivos locais são os fisicamente conectados ao computador. Os demais dispositivos que só podem ser acessados por conexões sem fio são chamados de dispositivos remotos.

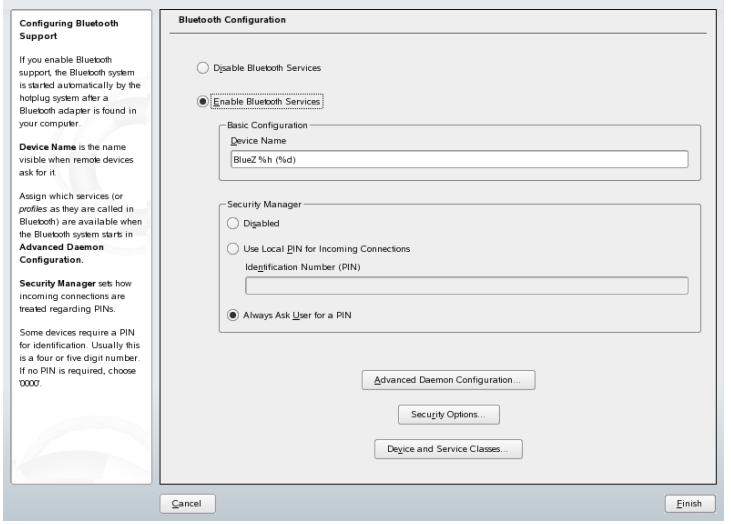
22.2.2 Configuração

Esta seção apresenta a configuração do Bluetooth. Saiba quais os arquivos de configuração envolvidos, que ferramentas são necessárias e como configurar o Bluetooth com YaST ou manualmente.

Configurando o Bluetooth com YaST

Use o módulo YaST do Bluetooth, mostrado em Figura 22.2, “Configuração YaST do Bluetooth” (p 317), para configurar o suporte do Bluetooth no sistema. Assim que o hotplug detectar um adaptador de Bluetooth no sistema (por exemplo, durante a inicialização ou quando você conectar um adaptador), o Bluetooth inicia automaticamente com as configurações desse módulo.

Figura 22.2 *Configuração YaST do Bluetooth*


Configuring Bluetooth Support
If you enable Bluetooth support, the Bluetooth system is started automatically by the hotplug system after a Bluetooth adapter is found in your computer.
Device Name is the name visible when remote devices ask for it.
Assign which services (or profiles as they are called in Bluetooth) are available when the Bluetooth system starts in Advanced Daemon Configuration.
Security Manager sets how incoming connections are treated regarding PINs.
Some devices require a PIN for identification. Usually this is a four or five digit number. If no PIN is required, choose '0000'.
Bluetooth Configuration
Disable Bluetooth Services
Enable Bluetooth Services
Basic Configuration
Device Name
BlueZ %h (%d)
Security Manager
Disabled
Use Local PIN for Incoming Connections
Identification Number (PIN)
Always Ask User for a PIN
Advanced Daemon Configuration...
Security Options...
Device and Service Classes...
Cancel
Finish

Na primeira etapa da configuração, determine se os serviços Bluetooth devem ser inicializados no sistema. Se tiver habilitado os serviços Bluetooth, dois itens podem ser configurados. Primeiro, o *Nome do Dispositivo*. É o nome que outros dispositivos exibem quando o seu computador tiver sido descoberto. Há dois marcadores de espaço disponíveis — `%h` significa o nome de host do sistema (útil, por exemplo, se foi atribuído dinamicamente por DHCP) e `%d` insere o número da interface (só é útil se você tiver mais de um adaptador Bluetooth no computador). Por exemplo, se você gravar `Laptop %h` no campo e DHCP atribuir o nome `unidade123` ao seu computador, outros dispositivos remotos reconheceriam o seu computador como `Laptop unidade123`.

O parâmetro *Gerenciador de Segurança* refere-se ao comportamento do sistema local quando um dispositivo remoto tenta se conectar. A diferença está no tratamento do número PIN. Permita que qualquer dispositivo se conecte sem um PIN ou, se o PIN for necessário, determine como o correto é escolhido. Você pode gravar um PIN (armazenado em um arquivo de configuração) no campo de entrada adequado. Se um dispositivo tentar se conectar, primeiro usa este PIN. Se falhar, ele recua para utilização sem PIN. Para máxima segurança, é melhor escolher *Solicitar PIN Sempre*. Esta opção permite que você use vários PINs para vários dispositivos (remotos).

Clique em *Configuração Daemon Avançada* para ativar a caixa de diálogo para selecionar e configurar os serviços disponíveis (chamados *perfis* no Bluetooth). Todos

os serviços disponíveis são exibidos em uma lista e podem ser habilitados ou desabilitados clicando em *Ativar* ou *Desativar*. Clique em *Editar* para abrir uma caixa de diálogo na qual especificar argumentos adicionais para o serviço selecionado (daemon). Não mude nada, a menos que conheça o serviço. Após concluir a configuração dos daemons, saia desta caixa de diálogo clicando em *OK*.

De volta à caixa de diálogo principal, clique em *Opções de Segurança* para abrir a caixa de diálogo de segurança e especificar criptografia, autenticação e configurações de exploração. Em seguida, saia da caixa de diálogo de segurança para retornar à caixa de diálogo principal. Após fechar a caixa de diálogo principal com *Concluir*, o sistema Bluetooth está pronto para uso.

Da caixa de diálogo principal, você também pode acessar a caixa de diálogo *Classes de Dispositivo e Serviço*. Os dispositivos Bluetooth são agrupados em várias classes de dispositivo. Nesta caixa de diálogo, escolha o correto para o seu computador, como *Desktop* ou *Laptop*. A classe de dispositivo não é muito importante, ao contrário da classe de serviço, também configurada aqui. Às vezes, dispositivos Bluetooth remotos, como telefones celulares, só aceitam determinadas funções se puderem detectar a classe de serviço correta configurada no sistema. Isso ocorre com freqüência com os telefones celulares que esperam uma classe chamada *Transferência de Objeto* antes de permitir a transferência dos arquivos de ou para o computador. Você pode escolher várias classes. Não é útil selecionar todas as classes "por via das dúvidas." A seleção padrão deve ser adequada na maioria dos casos.

Para usar o Bluetooth para configurar uma rede, ative *PAND* na caixa de diálogo *Configuração Daemon Avançada* e configure o modo do daemon com *Editar*. Para uma conexão de rede Bluetooth funcional, um pand deve operar no modo *Recepção* e o peer no modo *Pesquisar*. Por padrão, o modo *Recepção* é predefinido. Adapte o comportamento do seu pand local. Adicionalmente, configure a interface `bnepX` (`X` representa o número do dispositivo no sistema) no módulo YaST da*Placa de Rede*.

Configurando o Bluetooth manualmente

Os arquivos de configuração dos componentes individuais do sistema Bluez estão localizados no diretório `/etc/bluetooth`. A única exceção é o arquivo `/etc/sysconfig/bluetooth` para inicialização dos componentes, que é modificada pelo módulo YaST.

Os arquivos de configuração descritos abaixo só podem ser modificados pelo `root` do usuário. Atualmente, não há interface de usuário gráfico para mudar todas as

configurações. Os mais importantes podem ser configurados com o módulo YaST do Bluetooth, descrito em “Configurando o Bluetooth com YaST” (p 316). Todas as outras configurações só são do interesse de usuários experientes com casos especiais. Normalmente, as configurações padrão devem ser adequadas.

Um número PIN fornece proteção básica contra conexões indesejadas. Telefones móveis normalmente consultam o PIN quando estabelecem o primeiro contato (ou quando configuram um dispositivo de contato no telefone). Para que dois dispositivos possam se comunicar, ambos devem se identificar com o mesmo PIN. No computador, o PIN se localiza no arquivo `/etc/bluetooth/pin`.

IMPORTANTE: Segurança das conexões Bluetooth

Apesar dos PINs, a transmissão entre dois dispositivos pode não ser totalmente segura. Por padrão, a autenticação e a criptografia das conexões Bluetooth são desativadas. Ativar a autenticação e a criptografia pode resultar em problemas de comunicação com alguns dispositivos Bluetooth.

Várias configurações, como os nomes de dispositivo e o modo de segurança podem ser mudados no arquivo de configuração `/etc/bluetooth/hcid.conf`. Normalmente, as configurações padrão devem ser adequadas. O arquivo contém comentários descrevendo as opções para as diversas configurações.

Duas seções no arquivo incluído são designadas como `opções` e `dispositivo`. O primeiro contém informações gerais que hcid usa para iniciar. O último contém configurações para dispositivos Bluetooth individuais e locais.

Uma das configurações mais importantes da seção `opções` é `segurança autom tica`. Se configurado em `auto`, hcid tenta usar o PIN local para as conexões recebidas. Se falhar, alterna para `nenhum` e estabelece a conexão. Para maior segurança, esta configuração padrão deve ser definida para `usu rio` para verificar se o usuário é solicitado a digitar um PIN toda vez que uma conexão é estabelecida.

Configure o nome sob o qual o computador é exibido do outro lado na seção `dispositivo`. A classe de dispositivo, como `Desktop`, `Laptop` ou `Servidor` é definida nessa seção. Autenticação e criptografia também são habilitadas ou desabilitadas aqui.

22.2.3 Componentes e utilitários do sistema

A operabilidade do Bluetooth depende da interação de vários serviços. Pelo menos dois daemons em segundo plano são necessários: hcid (daemon da interface do controlador de host), que atua como interface para o dispositivo Bluetooth e o controla e sdpd (daemon de protocolo de discovery de serviços), por meio do qual um dispositivo pode descobrir que serviços o host torna disponível. Se não forem ativados automaticamente quando o sistema é inicializado, hcid e sdpd podem ser ativados com o comando `rcbluetooth start`. Este comando deve ser executado como `root`.

Os parágrafos a seguir descrevem resumidamente as ferramentas shell mais importantes que podem ser usadas para trabalhar com o Bluetooth. Embora vários componentes gráficos sejam agora disponíveis para controlar o Bluetooth, pode ser válido verificar esses programas.

Alguns dos comandos só podem ser executados como `root`. Entre eles o comando `l2ping` *`device_address`* para testar a conexão a um dispositivo remoto.

hcitool

hcitool pode ser usado para determinar se dispositivos locais e remotos são detectados. O comando `hcitool dev` lista os dispositivos locais. A saída gera uma linha na forma *`interface_name device_address`* para todo dispositivo local detectado.

Procure dispositivos remotos com o comando `hcitool inq`. Três valores retornam para todo dispositivo detectado: o endereço do dispositivo, a diferença de relógio e a classe de dispositivo. O endereço do dispositivo é importante, porque outros comandos o usam para identificar o dispositivo de destino. A diferença de relógio serve principalmente para um propósito técnico. A classe especifica o tipo de dispositivo e o tipo de serviço como um valor hexadecimal.

O comando `hcitool name` *`device-address`* pode ser usado para determinar o nome do dispositivo de um dispositivo remoto. No caso de um computador remoto, a classe e o nome do dispositivo correspondem às informações em seu `/etc/bluetooth/hcid.conf`. Endereços de dispositivo local geram uma saída de erro.

hciconfig

O comando `/usr/sbin/hciconfig` envia mais informações sobre o dispositivo local. Se `hciconfig` for executado sem quaisquer argumentos, a saída mostra informações do dispositivo, como o nome do dispositivo (`hciX`), o endereço do dispositivo físico (um número de 12 dígitos no formato `00:12:34:56:78`) e informações sobre a quantidade de dados transmitida.

`hciconfig hci0 name` exibe o nome que é retornado pelo seu computador quando recebe solicitações de dispositivos remotos. Assim como consultar as configurações do dispositivo local, `hciconfig` pode ser usado para modificar essas configurações. Por exemplo, `hciconfig hci0 name TEST` configura o nome em `TEST`.

sdptool

O programa sdptool pode ser usado para verificar que serviços se tornam disponíveis por um dispositivo específico. O comando `sdptool browse` *`device_address`* retorna todos os serviços de um dispositivo. Use o comando `sdptool search` *`service_code`* para procurar um serviço específico. Este comando digitaliza todos os dispositivos acessíveis para o serviço solicitado. Se um dos dispositivos oferecer o serviço, o programa imprime o nome completo do serviço retornado pelo dispositivo com uma breve descrição. Veja uma lista de todos os códigos de serviço possíveis digitando `sdptool` sem parâmetros.

22.2.4 Aplicativos gráficos

Em Konqueror, digite o URL `bluetooth:/` para listar dispositivos Bluetooth locais e remotos. Clique duas vezes em um dispositivo para obter uma visão geral dos serviços fornecidos pelo dispositivo. Se você mover por um dos serviços especificados com o mouse, a barra de status do browser mostra que perfil é usado para o serviço. Se você clicar em um serviço, uma caixa de diálogo é aberta, perguntando o que fazer: salvar, usar o serviço (deve ser iniciado um aplicativo para fazer isto) ou cancelar a ação. Marque uma caixa de seleção se não quiser que a caixa de diálogo seja exibida novamente mas quer que a ação selecionada seja realizada. Para alguns serviços, o suporte ainda não está disponível. Para outros, pode ser necessário instalar pacotes adicionais.

22.2.5 Exemplos

Esta seção oferece dois exemplos típicos de possíveis cenários Bluetooth. O primeiro mostra como uma conexão de rede entre dois hosts pode ser estabelecida através do Bluetooth. O segundo apresenta uma conexão entre um computador e um telefone móvel.

Conexão de rede entre dois hosts

No primeiro exemplo, é estabelecida uma conexão de rede entre os hosts *H1* e *H2*. Estes dois hosts têm endereços do dispositivo Bluetooth *baddr1* e *baddr2* (determinado nos dois hosts com o comando `hcitool dev` como descrito acima). Os hosts devem ser identificados com os endereços IP `192.168.1.3` (*H1*) e `192.168.1.4` (*H2*).

A conexão Bluetooth é estabelecida com a ajuda de pand (daemon de personal area network). Os seguintes comandos devem ser executados pelo usuário `root`. A descrição enfoca as ações específicas do Bluetooth e não fornece uma explicação detalhada do comando de rede `ip`.

Digite `pand -s` para iniciar pand no host *H1*. Em seguida, uma conexão pode ser estabelecida no host *H2* com `pand -c` *`baddr1`*. Se você digitar `ip link show` em um dos hosts para listar as interfaces de rede disponíveis, a saída deve conter uma entrada como a seguinte:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

Em vez de `00:12:34:56:89:90`, a saída deve conter o endereço do dispositivo local *baddr1* ou *baddr2*. Agora é necessário atribuir e ativar um endereço IP a esta interface. Em *H1*, isso pode ser feito com os dois comandos seguintes:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

Em *H2*:

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Agora *H1* pode ser acessado de *H2* com o IP `192.168.1.3`. Use o comando `ssh 192.168.1.4` para acessar *H2* de *H1*, supondo que *H2* executa um sshd, que é ativado

por padrão no SUSE Linux. O comando `ssh 192.168.1.4` também pode ser executado como um usuário normal.

Transferência de dados de um telefone móvel para o computador

O segundo exemplo mostra como transferir uma fotografia criada em um telefone móvel com uma câmara digital interna para um computador (sem incorrer em custos adicionais para a transmissão de uma mensagem multimídia). Embora a estrutura do menu possa ser diferente em vários telefones móveis, o procedimento geralmente é bastante semelhante. Consulte o manual do seu telefone, se necessário. Este exemplo descreve a transferência de uma fotografia de um telefone móvel Sony Ericsson para um laptop. O serviço Obex-Push deve estar disponível no computador e o computador deve conceder acesso ao telefone móvel. Na primeira etapa, o serviço se torna disponível no laptop. Isto é feito através do opd daemon do pacote `bluez-utils`. Inicie o daemon com o seguinte comando:

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

São usados dois importantes parâmetros: `--sdp` registra o serviço com sdpd e `--path /tmp` instrui o programa onde salvar os dados recebidos, neste caso em `/tmp`. Você também pode especificar qualquer outro diretório ao qual tenha acesso de gravação.

Agora o telefone móvel deve reconhecer o computador. Para isso, abra o menu *Conectar* no telefone e selecione *Bluetooth*. Se necessário, clique em *Ativar* antes de selecionar *Meus dispositivos*. Selecione *Novo dispositivo* e deixe o seu telefone procurar o laptop. Se um dispositivo for detectado, o nome aparecerá na tela. Selecione o dispositivo associado ao laptop. Se encontrar uma consulta de PIN, digite o PIN especificado em `/etc/bluetooth/pin`. Agora o seu telefone reconhece o laptop e é capaz de trocar dados com o laptop. Saia do menu atual e vá para o menu da imagem. Selecione a imagem a transferir e pressione *Mais*. No menu seguinte, pressione *Enviar* para selecionar um modo de transmissão. Selecione *Via Bluetooth*. O laptop deve ser listado como dispositivo de destino. Selecione o laptop para iniciar a transmissão. A imagem é então salva no diretório especificado com o comando `opd` . Faixas de áudio podem ser transferidas para o laptop da mesma maneira.

22.2.6 Solução de problemas

Se tiver dificuldades em estabelecer uma conexão, prossiga de acordo com a seguinte lista. Lembre-se de que o erro pode estar de um lado da conexão ou mesmo de ambos. Se possível, reconstrua o problema com outro dispositivo Bluetooth para verificar se o dispositivo não está com defeito.

O dispositivo local está listado na saída do `hcitool dev`?
Se o dispositivo local não estiver listado nesta saída, hcid não é iniciado ou o dispositivo não é reconhecido como um dispositivo Bluetooth. Isto pode ter várias causas. O dispositivo pode estar com defeito ou o driver correto pode estar faltando. Laptops com Bluetooth interno em geral têm um switch de ativar e desativar para dispositivos sem fio, como WLAN e Bluetooth. Consulte o manual do laptop para ver se o seu dispositivo tem este switch. Reinicie o sistema Bluetooth com o comando `rcbluetooth restart` e verifique se há erros reportados em `/var/log/messages`.

O seu adaptador Bluetooth precisa de um arquivo firmware?
Nesse caso, instale `bluez-bluefw` e reinicie o sistema Bluetooth com `rcbluetooth restart`.

A saída de `hcitool inq` retorna outros dispositivos?
Teste este comando mais de uma vez. A conexão pode ter interferências, porque a banda da freqüência do Bluetooth já é usada por outros dispositivos.

Os PINs correspondem?
Verifique se o número PIN do computador (em `/etc/bluetooth/pin`) corresponde ao do dispositivo de destino.

O dispositivo remoto pode "ver" o seu computador?
Tente estabelecer a conexão do dispositivo remoto. Verifique se este dispositivo vê o computador.

A conexão de rede pode ser estabelecida (veja "Conexão de rede entre dois hosts" (p 322))?
A configuração descrita em "Conexão de rede entre dois hosts" (p 322) pode não funcionar por várias razões. Por exemplo, um dos dois computadores pode não ter suporte para o protocolo ssh. Tente `ping 192.168.1.3` ou `ping 192.168.1.4`. Se funcionar, verifique se sshd está ativo. Outro problema pode ser que um dos dois dispositivo já possui configurações de rede que conflitam com

o endereço `192.168.1.X` do exemplo. Se for o caso, tente vários endereços, como `10.123.1.2` e `10.123.1.3`.

O laptop parece um dispositivo de destino (consulte "Transferência de dados de um telefone móvel para o computador" (p 323))? O dispositivo móvel reconhece o serviço Obex-Push no laptop?

Em *Meus dispositivos*, selecione o respectivo dispositivo e veja a lista de *Serviços*. Se Obex-Push não for exibido (mesmo depois da atualização da lista), o problema é causado por opd no laptop. O opd está ativo? Você tem acesso de gravação ao diretório especificado?

O cenário descrito em "Transferência de dados de um telefone móvel para o computador" (p 323) funciona na direção contrária?

Se o pacote `obexftp` estiver instalado, o comando `obexftp -b` *`device_address`* `-B 10 -p` *`image`* pode ser usado em alguns dispositivos. Vários modelos Siemens e Sony Ericsson foram testados e demonstraram ser funcionais. Consulte a documentação em `/usr/share/doc/packages/obexftp`.

22.2.7 Para obter mais informações

Uma ampla visão geral de várias instruções para o uso e a configuração do Bluetooth está disponível em `http://www.holtmann.org/linux/bluetooth/`. Outras informações e instruções úteis:

- Documentação HOWTO oficial sobre a pilha de protocolos Bluetooth integrada ao kernel: `http://bluez.sourceforge.net/howto/index.html`
- Conexão para PalmOS PDA: `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

22.3 Transmissão de dados infravermelhos

A IrDA (Infrared Data Association - Associação de Dados Infravermelhos) é um padrão da indústria para comunicação sem fio com luz infravermelha. Muitos laptops vendidos

atualmente são equipados com um transceptor compatível com IrDA que permite a comunicação com outros dispositivos, como impressoras, modems, LANs ou outros laptops. A velocidade de transferência varia de 2.400 bps a 4 Mbps.

Há dois modos de operação IrDA. O modo padrão, SIR, acessa a porta infravermelha por meio de uma interface serial. Esse modo funciona em quase todos os sistemas, sendo suficiente para a maioria dos requisitos. O modo mais rápido, FIR, requer um driver especial para o chip do IrDA. Nem todos os tipos de chip são suportados no modo FIR, devido à ausência de drivers apropriados. Defina o modo de IrDA desejado no BIOS de seu computador. O BIOS também mostra que interface serial é usada no modo SIR.

É possível encontrar informações sobre o IrDA no guia do IrDA da Werner Heuser, em `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html`. Além disso, consulte o site da Web do Projeto IrDA do Linux, em `http://irda.sourceforge.net/`.

22.3.1 Software

Os módulos de kernel necessários são incluídos no pacote do kernel. O pacote `irda` fornece os aplicativos ajudantes necessários para suportar a interface infravermelha. A documentação pode ser encontrada em `/usr/share/doc/packages/irda/README`, depois da instalação do pacote.

22.3.2 Configuração

O serviço do sistema IrDA não é iniciado automaticamente quando o sistema é iniciado. Use o módulo IrDA do YaST para a ativação. Só é possível modificar uma configuração neste módulo: a interface serial do dispositivo infravermelho. A janela de teste mostra duas saídas. Uma é a saída de `irdadump`, que registra todos os pacotes de IrDA enviados e recebidos. Essa saída deve conter o nome do computador e os nomes de todos os dispositivos infravermelhos da faixa de transmissão. Há um exemplo dessas mensagens na Seção 22.3.4, “Solução de problemas” (p 328). Todos os dispositivos para os quais existe uma conexão IrDA são relacionados na parte inferior da janela.

O IrDA consome uma quantidade considerável de energia da bateria, pois pacotes de descoberta são enviados com um intervalo de poucos segundos para detectar outros dispositivos periféricos. Portanto, caso você dependa da energia da bateria, o IrDA só

deverá ser iniciado quando necessário. Digite o comando `rcirda start` para ativá-lo ou `rcirda stop` para encerrá-lo. Todos os módulos de kernel necessários serão carregados automaticamente quando a interface for ativada.

A configuração manual pode ser executada no arquivo `/etc/sysconfig/irda`. O arquivo contém apenas uma variável, `IRDA_PORT`, que determina a interface a ser usada no modo SIR.

22.3.3 Uso

Os dados podem ser enviados para o arquivo de dispositivo `/dev/irlpt0` para impressão. O arquivo do dispositivo `/dev/irlpt0` age como a interface cabeada `/dev/lp0` normal, sendo que os dados de impressão são enviados em modo sem fio com a luz infravermelha. Para imprimir, verifique se a impressora está dentro da faixa visual da interface infravermelha do computador e se o suporte a infravermelho foi iniciado.

Uma impressora operada pela interface infravermelha pode ser configurada com o módulo Impressora do YaST. Como ela não é detectada automaticamente, configure-a manualmente clicando em *Outro (não detectado)*. Na caixa de diálogo seguinte, selecione *Impressora IrDA*. Normalmente, a conexão correta é `irlpt0`. Os detalhes sobre as impressoras em operação no Linux estão disponíveis no Capítulo 31, *Operação da impressora* (p 491).

A comunicação com outros hosts e com telefones celulares ou dispositivos semelhantes é conduzida por meio do arquivo de dispositivo `/dev/ircomm0`. Os telefones celulares Siemens S25 e Nokia 6210, por exemplo, podem discar e se conectar com a Internet com o aplicativo wvdial, usando a interface infravermelha. A sincronização de dados com um Palm Pilot também é possível, desde que a configuração do dispositivo do aplicativo correspondente seja definida como `/dev/ircomm0`.

Se desejar, você poderá usar apenas dispositivos que suportem os protocolos da impressora ou IrCOMM. Dispositivos que suportam o protocolo IROBEX, como 3Com Palm Pilot, podem ser acessados com aplicativos especiais, como irobexpalm e irobexreceive. Consulte *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`) para obter mais informações. Os protocolos suportados pelo dispositivo são relacionados entre colchetes depois do nome do dispositivo, na saída de `irdadump`. O suporte ao protocolo rLAN ainda está “em andamento”.

22.3.4 Solução de problemas

Se os dispositivos conectados à porta infravermelha não responderem, use o comando `irdadump` (como `root`) para verificar se o outro dispositivo é reconhecido pelo computador. Algo semelhante ao Exemplo 22.1, “Saída de irdadump” (p 328) será exibido regularmente, quando uma impressora Canon BJC-80 estiver dentro de uma faixa visível do computador:

Exemplo 22.1 *Saída de irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                        hint=0500 [ PnP Computer ] (21)
```

Verifique a configuração da interface se não houver saída ou se o outro dispositivo não responder. Verifique se a interface correta está sendo usada. Algumas vezes, a interface infravermelha está localizada em `/dev/ttyS2` ou em `/dev/ttyS3`, e interrupções diferentes de IRQ 3 são usadas ocasionalmente. Essas configurações podem ser verificadas e modificadas no menu de configuração do BIOS de quase todos os laptops.

Uma simples câmera de vídeo também pode ajudar a determinar se o LED infravermelho está acendendo. A maioria das câmeras de vídeo pode ver a luz infravermelha, que nossos olhos não vêem.

Parte VII Administração

23 Segurança no Linux

O mascaramento e um firewall garantem um fluxo de dados e um intercâmbio de dados controlados. O SSH (secure shell) permite que você efetue login em hosts remotos por uma conexão criptografada. A criptografia de arquivos ou partições inteiras protege seus dados no caso de terceiros obterem acesso ao seu sistema. Encontre instruções técnicas e informações sobre aspectos de segurança das redes Linux.

23.1 Mascaramento e firewalls

Sempre que o Linux é usado em um ambiente de rede, você pode usar as funções de kernel que permitem a manipulação de pacotes de rede, para manter uma separação entre as áreas de rede interna e externa. O framework do filtro de rede do Linux oferece meios de estabelecer um firewall eficiente que mantém redes diferentes distanciadas. Com a ajuda de iptables, uma estrutura de tabela genérica para a definição de conjuntos de regras, controle precisamente os pacotes com permissão de passagem por uma interface de rede. Um filtro de pacote como esse pode ser configurado facilmente com a ajuda do SuSEfirewall2 e o módulo YaST correspondente.

23.1.1 Filtragem de pacotes com iptables

Os componentes netfilter e iptables são responsáveis pela filtragem e manipulação de pacotes de rede, assim como pela NAT (Network Address Translation - Conversão de Endereços de Rede). Os critérios de filtragem e quaisquer ações associadas a eles são armazenados em cadeias, que precisam estar relacionadas uma após a outra, por pacotes de rede individuais, à medida que forem chegando. As cadeias a serem relacionadas

são armazenadas em tabelas. O comando `iptables` permite alterar esses conjuntos regras e tabelas.

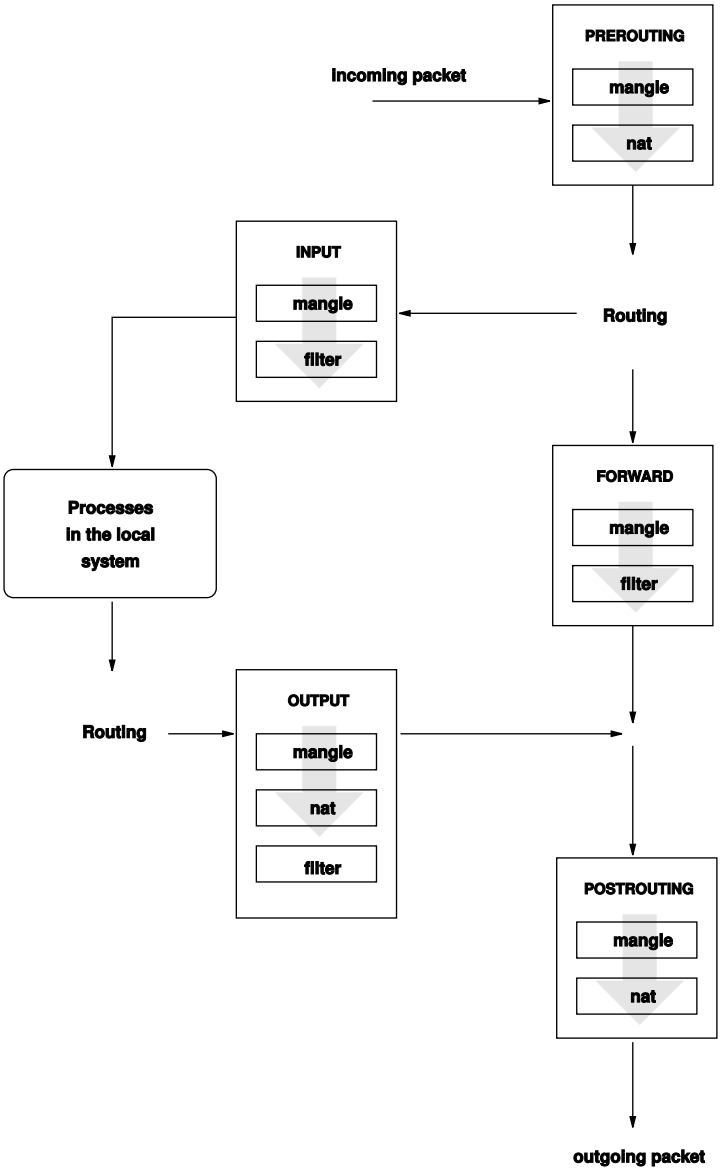
O kernel do Linux mantém três tabelas, cada qual para uma categoria de funções específicas do filtro do pacote:

filter
: Essa tabela contém o volume das regras do filtro, pois ele implementa o mecanismo de *filtragem de pacotes* em sentido restrito, que determina se os pacotes passam por (`ACCEPT`) ou se são descartados (`DROP`), por exemplo.

nat
: Essa tabela define quaisquer mudanças feitas nos endereços de origem e de destino dos pacotes. O uso dessas funções permite implementar um *mascaramento*, que é um caso especial da NAT, usado para vincular uma rede privada à Internet.

mangle
: As regras determinadas nessa tabela possibilitam manipular valores armazenados em cabeçalhos IP (como o tipo do serviço).

Figura 23.1 *iptables: Caminhos possíveis de um pacote*



Estas tabelas contêm várias cadeias predefinidas para relacionar pacotes:

PREROUTING
Esta cadeia é aplicada a pacotes recebidos.

INPUT
Esta cadeia é aplicada a pacotes destinados aos processos internos do sistema.

FORWARD
Esta cadeia é aplicada a pacotes roteados somente pelo sistema.

OUTPUT
Esta cadeia é aplicada a pacotes originados do próprio sistema.

POSTROUTING
Esta cadeia é aplicada a todos os pacotes enviados.

A Figura 23.1, “iptables: Caminhos possíveis de um pacote” (p 333) ilustra os caminhos pelos quais um pacote de rede pode viajar em um determinado sistema. Para manter a simplicidade, a figura lista tabelas como partes de cadeias. Contudo, na realidade, essas cadeias estão contidas nas próprias tabelas.

Em um dos casos mais simples possível, um pacote recebido destinado ao próprio sistema chega na interface `eth0`. Primeiro, o pacote é reconhecido pela cadeia `PREROUTING` da tabela `mangle` e, depois, na cadeia `PREROUTING` da tabela `nat`. A etapa a seguir, referente ao roteamento do pacote, determina que o destino real do pacote é um processo do próprio sistema. Depois de passar pelas cadeias `INPUT` das tabelas `mangle` e `filter`, o pacote por fim chega ao seu destino, desde que as regras da tabela `filter` tenham sido realmente relacionadas.

23.1.2 Informações básicas sobre mascaramento

Mascaramento é a forma específica do Linux para a NAT. Pode ser usado para conectar uma LAN pequena (em que hosts usam endereços IP da faixa privada — consulte a Seção 38.1.2, “Máscaras de rede e roteamento” (p 589)) à Internet (em que endereços IP oficiais são usados). Para que os hosts da LAN sejam capazes de se conectar à Internet, seus endereços privados são convertidos em um oficial. Isso é feito no roteador, que atua como gateway entre a LAN e a Internet. O princípio subjacente é bastante simples: o roteador possui mais de uma interface de rede, normalmente uma placa de rede e uma interface separada conectadas à Internet. Enquanto a última vincula o roteador

ao mundo externo, uma ou várias outras o vinculam-no aos hosts da LAN. Com esses hosts na rede local conectados à placa de rede (como o `eth0`) do roteador, eles podem enviar qualquer pacote não destinado à rede local para seus roteadores ou gateways padrão.

IMPORTANTE: Usando a máscara de rede correta

Ao configurar a rede, verifique se o endereço de broadcast e a máscara de rede são os mesmos para todos os hosts locais. Sem essa verificação, os pacotes poderão não ser roteados corretamente.

Conforme mencionado, sempre que um dos hosts da LAN enviar um pacote destinado a um endereço da Internet, ele irá para o roteador padrão. Entretanto, o roteador precisará estar configurado antes de encaminhar esse pacote. Por razões de segurança, o SUSE Linux não habilita essa função em sua instalação padrão. Para habilitá-la, configure a variável `IP_FORWARD` no arquivo `/etc/sysconfig/sysctl` para `IP_FORWARD=yes`.

O host de destino da conexão poderá ver o roteador, mas não saberá sobre o host da rede interna, do qual os pacotes são provenientes. Essa é a razão de a técnica ser chamada de mascaramento. Devido à conversão do endereço, o roteador é o primeiro destino de qualquer pacote de resposta. O roteador precisa identificar esses pacotes recebidos e converter seus endereços de destino, para que os pacotes possam ser encaminhados ao host correto na rede local.

Com o roteamento do tráfego de entrada, dependendo da tabela de mascaramento, não há como abrir uma conexão para um host interno pela parte externa. Para uma conexão como essa, não haveria entrada na tabela. Além disso, qualquer conexão já estabelecida possui uma entrada de status que lhe foi designada na tabela; portanto, a entrada não pode ser usada por outra conexão.

Como conseqüência de tudo isso, talvez você tenha alguns problemas com um número de protocolos de aplicativos, como ICQ, cucme, IRC (DCC, CTCP) e FTP (no modo PORTA). Netscape, o programa padrão de FTP, e muitos outros usam o modo PASV. Esse modo passivo é bem menos problemático, contanto que o mascaramento e a filtragem de pacotes estejam envolvidos.

23.1.3 Informações básicas sobre firewall

Firewall é, provavelmente, o termo mais amplamente usado para descrever um mecanismo que fornece e gerencia um link entre redes e, ao mesmo tempo, controla o fluxo de dados entre eles. Falando estritamente, o mecanismo descrito nesta seção é chamado de *filtro de pacote*. Um filtro de pacote regula o fluxo de dados de acordo com certos critérios, como protocolos, portas e endereços IP. Isso permite bloquear pacotes que, de acordo com seus respectivos endereços, não deveriam entrar em sua rede. Para permitir acesso público ao seu servidor Web, por exemplo, abra explicitamente a porta correspondente. Entretanto, um filtro de pacote não explora o conteúdo de pacotes com endereços legítimos, como aqueles direcionados para o servidor Web. Por exemplo, se pacotes recebidos tivessem a finalidade de comprometer um programa CGI no servidor Web, o filtro de pacote os deixaria entrar mesmo assim.

Um mecanismo mais eficiente, porém mais complexo, é a combinação de vários tipos de sistemas, como um filtro de pacote interagindo com um proxy ou gateway de aplicativo. Nesse caso, o filtro de pacote rejeita qualquer pacote destinado a portas desabilitadas. Somente pacotes direcionados ao gateway do aplicativo são aceitos. Esse gateway ou proxy finge ser o cliente real do servidor. De certo modo, tal proxy poderia ser considerado um host de mascaramento no nível de protocolo usado pelo aplicativo. Um exemplo desse proxy é o Squid, um servidor de proxy HTTP. Para usar o Squid, o browser precisa estar configurado para se comunicar através do proxy. Quaisquer páginas HTTP solicitadas são atendidas pelo cache do proxy e as não encontradas no cache são obtidas na Internet pelo proxy. Como exemplo adicional, o SUSE proxy-suite (`proxy-suite`) oferece um proxy para o protocolo FTP.

A seção a seguir enfoca o filtro de pacote que vem com o SUSE Linux. Para obter mais informações sobre firewall e filtragem de pacotes, leia o HOWTO do Firewall, incluído no pacote `howto`. Se esse pacote estiver instalado, leia o HOWTO com o `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz`.

23.1.4 SuSEfirewall2

O SuSEfirewall2 é um script que lê as variáveis configuradas em `/etc/sysconfig/SuSEfirewall2` para gerar um conjunto de regras iptables. Ele define três zonas de segurança, apesar de somente a primeira e a segunda serem consideradas na configuração de amostra a seguir:

Zona externa
: Considerando que não há como controlar o que ocorre na rede externa, os hosts precisam ser protegidos contra ela. Na maioria dos casos, a rede externa é a Internet, mas poderia ser outra rede sem segurança, como uma WLAN.

Zona interna
: Ela se refere à rede privada, normalmente, a LAN. Se os hosts dessa rede usam endereços IP do intervalo privado (consulte a Seção 38.1.2, “Máscaras de rede e roteamento” (p 589)), habilite a NAT, para que os hosts da rede interna possam acessar a externa.

DMZ (Demilitarized Zone - Zona Desmilitarizada)
: Apesar de os hosts localizados nessa zona poderem ser localizados tanto da rede externa quanto da interna, eles não conseguem acessar sozinhos a rede interna. Essa configuração pode ser usada para incluir uma linha adicional de defesa na frente da rede interna, pois os sistemas DMZ ficam isolados da rede interna.

Qualquer tipo de tráfego de rede não explicitamente permitido pelo conjunto de regras de filtragem é suprimido por iptables. Portanto, cada uma das interfaces com tráfego recebido precisa ser posicionada em uma das três zonas. Para cada uma das zonas, defina os serviços ou protocolos permitidos. O conjunto de regras é aplicado somente em pacotes originados de hosts remotos. Pacotes gerados localmente não são capturados pelo firewall.

A configuração pode ser executada com o YaST (consulte a “Configurando com o YaST” (p 337)). Também pode ser feita manualmente no arquivo `/etc/sysconfig/SuSEfirewall2`, que contém vários comentários. Além disso, vários cenários de exemplo estão disponíveis em `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES`.

Configurando com o YaST

IMPORTANTE: Configuração automática de firewall

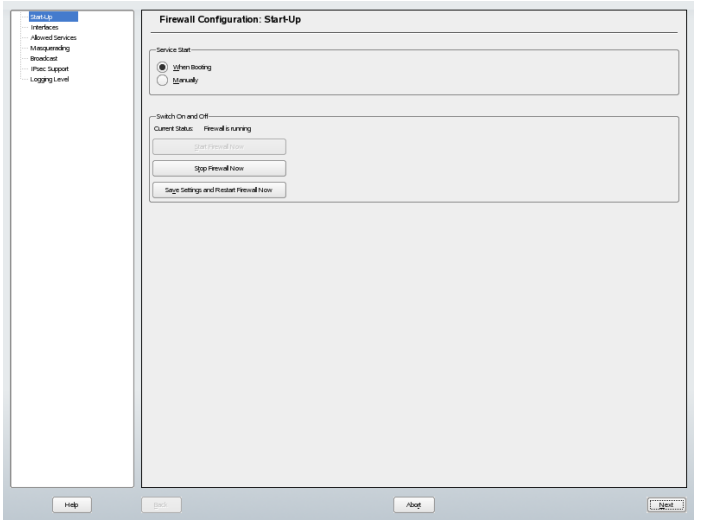
Depois da instalação, o YaST inicia um firewall automaticamente em todas as interfaces configuradas. Se um servidor for configurado e ativado no sistema, o YaST poderá modificar a configuração de firewall gerada automaticamente com as opções *Abrir Portas da Interface Selecionada no Firewall* ou *Abrir Portas no Firewall* nos módulos de configuração do servidor. Algumas caixas de diálogo

do módulo do servidor incluem o botão *Detalhes do Firewall* para ativar serviços e portas adicionais. O módulo de configuração de firewall do YaST pode ser usado para ativar, desativar ou reconfigurar o firewall.

As caixas de diálogo do YaST para a configuração gráfica podem ser acessadas no Centro de Controle do YaST. Selecione *Segurança e Usuários → Firewall*. A configuração é dividida em sete seções que podem ser acessadas diretamente da estrutura em árvore no lado esquerdo.

Inicialização
: Configure o comportamento de inicialização nesta caixa de diálogo. Em uma instalação padrão, o SUSEfirewall2 é iniciado automaticamente. Você também pode iniciar e parar o firewall aqui. Para implementar suas novas configurações em um firewall em execução, use *Salvar Configurações e Reiniciar Firewall Agora*.

Figura 23.2 *A configuração de firewall do YaST*



Interfaces
: Todas as interfaces de rede conhecidas estão listadas aqui. Para remover uma interface de uma zona, selecione-a, pressione *Modificar* e escolha *Nenhuma Zona Designada*. Para adicionar uma interface a uma zona, selecione-a, pressione *Modificar* e escolha qualquer das zonas disponíveis. Você também pode criar uma interface especial com suas próprias configurações usando *Personalizar*.

Serviços permitidos

Essa opção é necessária para oferecer serviços do seu sistema para uma zona da qual ele é protegido. Por padrão, o sistema é protegido somente de zonas externas. Permita, de forma explícita, os serviços que devem estar disponíveis para hosts externos. Ative os serviços após selecionar a zona desejada em *Serviços permitidos para zona selecionada*.

Mascaramento

O mascaramento oculta sua rede interna das redes externas, como a Internet, e habilita hosts na rede interna para acessarem a rede externa de forma transparente. As solicitações da rede externa para a interna são bloqueadas e as solicitações da rede interna parecem ser emitidas pelo servidor de mascaramento quando vistas externamente. Se serviços especiais de uma máquina interna precisarem estar disponíveis para a rede externa, adicione regras especiais de redirecionamento ao serviço.

Broadcast

Nessa caixa de diálogo, configure as portas UDP que permitem broadcasts. Adicione os serviços ou números de porta solicitados à zona apropriada, separados por espaços. Consulte também o arquivo `/etc/services`.

O registro de broadcasts não aceitos pode ser habilitado aqui. Isso pode ser problemático, pois os hosts do Windows usam broadcasts para sua identificação e, assim, geram muitos pacotes que não são aceitos.

Suporte a IPsec

Configure nesta caixa de diálogo se o serviço IPsec deve estar disponível para a rede externa. Configure quais pacotes são confiáveis em *Detalhes*.

Nível de registro

Há duas regras para o registro: pacotes aceitos e não aceitos. Pacotes não aceitos são DESCARTADOS ou REJEITADOS. Selecione *Registrar Tudo*, *Registrar Apenas Críticos* ou *Não Registrar Nenhum* para as duas opções.

Ao concluir a configuração do firewall, saia dessa caixa de diálogo com *Próximo*. Será aberto um resumo orientado por zona da configuração do firewall. Nele, verifique todas as configurações. Todos os serviços, portas e protocolos permitidos estão listados nesse resumo. Para modificar a configuração, use *Voltar*. Pressione *Aceitar* para gravar as configurações.

Configurando manualmente

Os parágrafos a seguir fornecem instruções passo a passo para executar uma configuração bem-sucedida. Cada item de configuração é marcado se é relevante para firewall ou para mascaramento. Os aspectos relacionados à DMZ, conforme mencionado no arquivo de configuração, não serão abordados aqui. Eles são aplicáveis somente a uma infra-estrutura de rede mais complexa, encontrada em organizações maiores (redes corporativas), que exigem uma configuração extensa e conhecimento profundo sobre o assunto.

Primeiro, use o módulo do YaST Serviços do Sistema (Nível de Execução) para habilitar o SuSEfirewall2 no seu nível de execução (provavelmente, 3 ou 5). Ele configura os symlinks para o SuSEfirewall2_* scripts nos diretórios `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (firewall, mascaramento)
: O dispositivo vinculado à Internet. Para obter uma conexão via modem, digite `ppp0`. Para obter um link ISDN, use o `ippp0`. As conexões DSL usam o `dsl0`. Especifique `auto` para usar a interface que corresponde à rota padrão.

`FW_DEV_INT` (firewall, mascaramento)
: O dispositivo vinculado à rede privada, interna (como a `eth0`). Deixe esse espaço vazio se não houver rede interna e o firewall protegerá somente o host em que estiver sendo executado.

`FW_ROUTE` (firewall, mascaramento)
: Se você precisar da função mascaramento, configure como `yes`. Os hosts internos não ficarão visíveis de fora, pois seus endereços de rede privada (por exemplo, `192.168.x.x`) serão ignorados pelos roteadores da Internet.

  Para um firewall sem mascaramento, configure como `yes` somente se desejar permitir acesso à rede interna. Os hosts internos precisam usar IPs registrados oficialmente nesse caso. No entanto, normalmente você *não* deveria permitir o acesso externo à sua rede interna.

`FW_MASQUERADE` (mascaramento)
: Configure como `yes`, se você precisar da função mascaramento. Com isso, você terá uma conexão praticamente direta com a Internet para os hosts internos. É mais seguro haver um servidor proxy entre os hosts da rede interna e a Internet. O mascaramento não é necessário para serviços fornecidos por um servidor proxy.

FW_MASQ_NETS (mascaramento)
Especifique as redes ou os hosts que devem ser mascarados, deixando um espaço entre as entradas individuais. Por exemplo:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (firewall)
Configure como `yes` e o host do firewall ficará protegido contra ataques que surgirem em sua rede interna. Os serviços só estarão disponíveis para a rede interna se estiverem explicitamente habilitados. Consulte também os serviços `FW_SERVICES_INT_TCP` e `FW_SERVICES_INT_UDP`.

FW_SERVICES_EXT_TCP (firewall)
Digite as portas TCP que devem ficar disponíveis. Deixe esse espaço vazio para uma estação de trabalho residencial normal, que não deve oferecer serviços.

FW_SERVICES_EXT_UDP (firewall)
Deixe esse espaço vazio, a menos que você execute um serviço UDP e deseje disponibilizá-lo externamente. Os serviços que usam o UDP incluem os servidores DNS, IPSec, TFTP, DHCP e outros. Nesse caso, digite as portas UDP a serem usadas.

FW_SERVICES_INT_TCP (firewall)
Com essa variável, defina os serviços disponíveis para a rede interna. A notação é a mesma do `FW_SERVICES_EXT_TCP`, mas as configurações são aplicadas à rede *interna*. A variável só precisará ser configurada se o `FW_PROTECT_FROM_INT` estiver configurado como `yes`.

FW_SERVICES_INT_UDP (firewall)
Consulte o FW_SERVICES_INT_TCP.

Depois de configurar o firewall, teste sua configuração. Os conjuntos de regras de firewall são criados digitando `SuSEfirewall2 start` como `root`. Depois, use `telnet`, por exemplo, de um host externo para ver se a conexão foi realmente negada. Depois disso, reveja `/var/log/messages`, em que deverá aparecer algo semelhante a:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

Outros pacotes que testam a configuração de um firewall são o nmap ou o nessus. A documentação do nmap pode ser encontrada em `/usr/share/doc/packages/nmap` e a do nessus no diretório `/usr/share/doc/packages/nessus-core` depois que o respectivo pacote estiver instalado.

23.1.5 Para obter mais informações

As informações mais recentes e outras documentações sobre o pacote `SuSEfirewall2` podem ser encontradas em `/usr/share/doc/packages/SuSEfirewall2`. A home page do projeto iptables e netfilter, `http://www.netfilter.org`, oferece uma grande coleção de documentos em vários idiomas.

23.2 SSH: operações seguras de rede

Com cada vez mais computadores instalados em ambientes de rede, sempre torna-se necessário acessar hosts de um local remoto. Isso normalmente significa que um usuário envia strings de login e senha para fins de autenticação. Como essas strings são transmitidas como texto simples, elas podem ser interceptadas e usadas de forma incorreta para obter acesso à conta do usuário sem que o usuário autorizado sequer saiba disso. Além da possibilidade de todos os arquivos do usuário serem abertos por um invasor, a conta ilegal pode ser usada para obter acesso de administrador ou `root`, ou para penetrar em outros sistemas. Anteriormente, as conexões remotas eram estabelecidas com telnet, que não oferece proteção contra espionagem na forma de criptografia nem de outros mecanismos de segurança. Há outros canais de comunicação sem proteção, como o tradicional protocolo FTP e alguns programas de cópia remotos.

A suíte do SSH fornece a proteção necessária, criptografando as strings de autenticação (normalmente um nome de login e uma senha) e todos os outros dados que sofrem intercâmbio nos hosts. Com o SSH, o fluxo de dados ainda pode ser registrado por terceiros, mas o conteúdo é criptografado e não pode ser revertido em texto simples, a menos que a chave de criptografia seja conhecida. Dessa forma, o SSF permite a comunicação segura em redes desprotegidas, como a Internet. O padrão de SSH que vem com o SUSE Linux é o OpenSSH.

23.2.1 Pacote OpenSSH

O SUSE Linux instala o pacote OpenSSH por padrão. Os programas ssh, scp e sftp são alternativas disponíveis ao telnet, rlogin, rsh, rcp e ftp. Na configuração padrão, o acesso a um sistema SUSE Linux só é possível com os utilitários do OpenSSH e somente se o firewall permitir acesso.

23.2.2 Programa ssh

Usando o programa ssh, é possível fazer login em sistemas remotos e trabalhar de forma interativa. Ele substitui o telnet e o rlogin. O programa slogin é apenas um link simbólico para o ssh. Por exemplo, efetue login no host sun com o comando `ssh sun`. O host solicita a senha para o sun.

Depois da autenticação bem-sucedida, você pode trabalhar na linha de comando remota ou usar aplicativos interativos, como o YaST. Se o nome de usuário local for diferente do nome de usuário remoto, você poderá efetuar login usando um nome de login diferente, com `ssh -l augustine sun`, ou `ssh augustine@sun`.

Além disso, o ssh oferece a possibilidade de executar comandos em sistemas remotos, como conhecido no rsh. No exemplo a seguir, execute o comando `uptime` no host sun e crie um diretório com o nome `tmp`. A saída do programa será exibida no terminal local do host earth.

```
ssh otherplanet "uptime; mkdir tmp"
tux@otherplanet's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

As aspas são necessárias aqui para enviar as duas instruções com um comando. Somente com esse procedimento o segundo comando é executado no sun.

23.2.3 scp (Secure Copy - Cópia Segura)

O scp copia arquivos em uma máquina remota. Ele é um substituto seguro e criptografado para o rcp. Por exemplo, `scp MyLetter.tex sun:` copia o arquivo `MyLetter.tex` do host earth para o host sun. Se o nome de usuário do earth for diferente do nome de usuário do sun, especifique o do sun usando o formato `username@host`. Não há opção `-l` para esse comando.

Depois que a senha correta é digitada, o scp inicia a transferência de dados e mostra uma linha crescente de asteriscos para simular uma barra de progresso. Além disso, o programa exibe o tempo estimado de chegada à direita da barra de progresso. Suprima toda a saída fornecendo a opção `-q`.

O scp também fornece um recurso de cópia recursiva para diretórios inteiros. O comando `scp -r src/ sun:backup/` copia todo o conteúdo do diretório `src`, incluindo todos os subdiretórios, no diretório `backup` do host sun. Se esse subdiretório ainda não existir, ele será criado automaticamente.

A opção `-p` avisa ao scp para não mudar a marcação de horário dos arquivos. A opção `-C` compacta a transferência de dados. Assim o volume de dados a ser transferido é minimizado, embora seja criada uma carga mais pesada para o processador.

23.2.4 sftp (Secure File Transfer - Transferência Segura de Arquivos)

O programa sftp pode ser usado como alternativa ao scp para a transferência segura de arquivos. Durante uma sessão do sftp, você pode usar muitos comandos conhecidos do ftp. O programa sftp pode ser uma alternativa melhor ao scp, especialmente na transferência de dados em que os nomes de arquivos são desconhecidos.

23.2.5 Daemon SSH (sshd) - executado no servidor

Para trabalhar com os programas clientes do SSH ssh e scp, o servidor daemon SSH deve estar em execução em segundo plano, escutando conexões `na porta TCP/IP 22`. O daemon garante três pares de chaves quando é iniciado pela primeira vez. Cada par de chaves consiste em uma chave privada e uma pública. Portanto, esse procedimento é conhecido como baseado em chave pública. Para garantir a segurança da comunicação via SSH, o acesso a arquivos de chave privada deve ser restrito ao administrador do sistema. As permissões de arquivos são definidas adequadamente pela instalação padrão. As chaves privadas só são exigidas localmente pelo daemon SSH e não devem ser fornecidas a ninguém mais. Os componentes da chave pública (reconhecidos pela extensão de nome `.pub`) são enviados para o cliente que solicita a conexão. Todos os usuários podem lê-los.

O cliente SSH inicia uma conexão. O daemon SSH e o cliente SSH que solicitou a conexão fazem um intercâmbio de dados de identificação para comparar as versões de software e o protocolo, e para evitar conexões pela porta errada. Como um processo filho do daemon SSH original responde à solicitação, várias conexões de SSH podem ser feitas ao mesmo tempo.

Para a comunicação entre o servidor SSH e o cliente SSH, o OpenSSH suporta as versões 1 e 2 do protocolo SSH. Os sistemas SUSE Linux recentes têm a versão 2 como padrão. Para continuar usando a versão 1 depois de uma atualização, siga as instruções de `/usr/share/doc/packages/openssh/README.SuSE`. Este documento também descreve como um ambiente SSH 1 pode ser transformado em um ambiente de trabalho SSH 2 em apenas algumas etapas.

Ao usar a versão 1 do SSH, o servidor envia sua chave pública de host e uma chave de servidor, que é gerada novamente pelo daemon SSH a cada hora. Ambas permitem que o cliente SSH criptografe uma chave de sessão escolhida livremente, que é enviada ao servidor SSH. O cliente SSH também comunica ao servidor qual método de criptografia (cifra) deve ser usado.

A versão 2 do protocolo de SSH não requer uma chave de servidor. Os dois lados usam um algoritmo de acordo com Diffie-Helman para fazer o intercâmbio de suas chaves.

O host privado e as chaves do servidor são absolutamente necessários para descriptografar a chave da sessão e não podem ser derivados de partes públicas. Somente o daemon SSH contatado pode descriptografar a chave da sessão usando suas chaves privadas (consulte `man /usr/share/doc/packages/openssh/RFC.nroff`). Essa fase inicial de conexão pode ser observada de perto, se você ativar a opção de depuração verbosa `-v` do cliente SSH.

A versão 2 do protocolo SSH é usada por padrão. Substitua-a pela versão 1 do protocolo com o switch `-1`. O cliente armazena todas as chaves públicas do host no arquivo `~/.ssh/known_hosts` depois de seu primeiro contato com um host remoto. Esse procedimento evita ataques man-in-the-middle (MITM) - tentativas de servidores SSH estrangeiros usarem nomes e endereços IP falsos. Esses ataques são detectados por uma chave de host não incluída em `~/.ssh/known_hosts` ou pela incapacidade do servidor de descriptografar a chave da sessão na ausência de um correlativo privado apropriado.

É recomendável fazer backup das chaves públicas e privadas armazenadas em `/etc/ssh/` em um local externo seguro. Desta forma, as modificações das chaves podem

ser detectadas e as chaves antigas podem ser usadas novamente depois de uma reinstalação. Esse procedimento poupa os usuários de avisos de desproteção. Verificou-se que, apesar do aviso - na realidade trata-se do servidor SSH correto -, a entrada para o sistema existente deve ser removida de `~/.ssh/known_hosts`.

23.2.6 Mecanismos de autenticação do SSH

Agora é hora da verdadeira autenticação, que, em sua forma mais simples, consiste na digitação de uma senha, conforme mencionado anteriormente. A meta do SSH é apresentar um software seguro que também seja fácil de usar. Como ele deve substituir o rsh e o rlogin, o SSH também deve ser capaz de fornecer um método de autenticação apropriado para uso diário. O SSH consegue isso por meio de outro par de chaves, gerado pelo usuário. O pacote do SSH fornece um programa de auxílio para isso: ssh-keygen. Depois da digitação de `ssh-keygen -t rsa` ou `ssh-keygen -t dsa`, o par de chaves é gerado e você deverá informar o nome do arquivo básico em que as chaves serão armazenadas.

Confirme a configuração padrão e responda à solicitação de uma frase secreta. Mesmo se o software sugerir que a frase secreta fique em branco, é recomendável inserir um texto de 10 a 30 caracteres para o procedimento descrito aqui. Não use palavras e frases curtas e simples. Confirme a frase secreta repetindo-a. Depois, você verá o local de armazenamento das chaves pública e privada, neste exemplo os arquivos `id_rsa` e `id_rsa.pub`.

Use `ssh-keygen -p -t rsa` ou `ssh-keygen -p -t dsa` para mudar sua frase secreta antiga. Copie o componente da chave pública (`id_rsa.pub`, no exemplo) na máquina remota e salve-o como `~/.ssh/authorized_keys`. Você será solicitado a autenticar-se com sua frase secreta na próxima vez em que estabelecer uma conexão. Se isso não ocorrer, verifique o local e o conteúdo desses arquivos.

A longo prazo, esse procedimento será mais importuno do que fornecer sempre a senha. Portanto, o pacote do SSH fornece outra ferramenta, o ssh-agent, que mantém as chaves privadas durante uma sessão X. Toda a sessão X é iniciada como um processo-filho do ssh-agent. A forma mais fácil de fazer isso é definir a variável `usessh` no começo do arquivo `.xsession` como `yes` e efetuar login por meio de um gerenciador de vídeo, como o KDM ou o XDM. Como alternativa, digite `ssh-agent startx`.

Agora você pode usar o ssh ou o scp como de costume. Se tiver distribuído sua chave pública como descrito acima, não será mais solicitado a informar sua senha. Fique

atento para concluir a sessão X ou bloqueá-la com um aplicativo de proteção de senha, como o xlock.

Todas as mudanças relevantes resultantes do lançamento da versão 2 do protocolo SSH também estão documentadas no arquivo `/usr/share/doc/packages/openssh/README.SuSE`.

23.2.7 X, autenticação e mecanismos de encaminhamento

Além das melhorias relativas a segurança descritas anteriormente, o SSH também simplifica o uso dos aplicativos X remotos. Se você executar `ssh` com a opção `-X`, a variável DISPLAY será automaticamente definida na máquina remota, e todas as saídas X serão exportadas para a máquina remota pela conexão SSH existente. Ao mesmo tempo, os aplicativos X iniciados remotamente e visualizados localmente com esse método não poderão ser interceptados por pessoas sem autorização.

Com a adição da opção `-A`, o mecanismo de autenticação ssh-agent passa para a próxima máquina. Dessa forma, você poderá trabalhar em máquinas diferentes sem precisar digitar a senha, mas somente se tiver distribuído sua chave pública nos hosts de destino e a gravado adequadamente neles.

Os dois mecanismos são desativados nas configurações padrão, mas podem ser ativados de forma permanente a qualquer momento no arquivo de configuração de todo o sistema `/etc/ssh/sshd_config` ou pelo `~/.ssh/config` do usuário.

O ssh também pode ser usado para redirecionar conexões TCP/IP. Nos exemplos abaixo, o SSH foi configurado para redirecionar as portas SMTP e POP3, respectivamente.

```
ssh -L 25:sun:25 earth
```

Com esse comando, qualquer conexão direcionada para a porta 25 (SMTP) do earth é redirecionada para a porta SMTP do sun por meio de um canal criptografado. Esse recurso é especialmente útil para os que usam servidores SMTP sem os recursos SMTP-AUTH ou POP-before-SMTP. De qualquer local arbitrário conectado a uma rede, é possível transferir e-mails para o servidor de correio eletrônico "doméstico" para entrega. Da mesma forma, todas as solicitações de POP3 (porta 110) do earth podem ser encaminhadas para a porta POP3 do sun com esse comando.

```
ssh -L 110:sun:110 earth
```

Os dois comandos devem ser executados como `root`, pois a conexão é feita para portas locais privilegiadas. Os e-mails são enviados e recuperados por usuários normais em uma conexão SSH existente. Os hosts SMTP e POP3 devem ser definidos como `localhost` para que isso funcione. Outras informações podem ser encontradas nas páginas de manual referentes a cada programa descrito acima, bem como nos arquivos em `/usr/share/doc/packages/openssh`.

23.3 Criptografando partições e arquivos

Todo usuário tem alguns dados confidenciais que não devem ser acessados por terceiros. Quanto mais abrangentes forem sua conexão e mobilidade, mais cuidado você deve ter para tratar seus dados. A criptografia de arquivos ou de partições inteiras será recomendável se outras pessoas tiverem acesso por uma conexão de rede ou acesso físico direto.

ATENÇÃO: A mídia criptografada é uma proteção limitada

Lembre-se de que, com os métodos descritos nesta seção, você não pode impedir que seu sistema em execução seja comprometido. Após a montagem da mídia criptografada, todas as pessoas com permissões adequadas terão acesso a ela. A mídia criptografada será útil se você perder seu computador ou se ele for roubado e pessoas não autorizadas quiserem ler seus dados confidenciais.

A lista a seguir apresenta diversos cenários de uso imagináveis.

Laptops
: Se você levar seu laptop em uma viagem, é uma boa idéia criptografar as partições do disco rígido que contenham dados confidenciais. Se você perder o laptop ou se ele for roubado, seus dados ficarão fora de alcance se residirem em um sistema de arquivos criptografado ou em um único arquivo criptografado.

Mídia removível
: Unidades flash USB ou discos rígidos externos são tão suscetíveis a roubo quanto laptops. Um sistema de arquivos criptografado fornece proteção contra o acesso de terceiros.

Estações de trabalho

Em empresas nas quais quase todas as pessoas têm acesso ao seu computador, pode ser útil criptografar a partição ou arquivos individuais.

23.3.1 Configurando um sistema de arquivos criptografado com o YaST

O YaST permite a criptografia de arquivos ou partições durante a instalação, bem como em um sistema já instalado. É possível criar um arquivo criptografado a qualquer momento, pois ele se ajusta perfeitamente ao layout de uma partição existente. Para criptografar uma partição inteira, separe uma no layout de partições. A proposta padrão de particionamento, como sugerida pelo YaST, não inclui por padrão uma partição criptografada. Adicione-a manualmente na caixa de diálogo de particionamento.

Criando uma partição criptografada durante a instalação

ATENÇÃO: Entrada de senha

Observe os avisos sobre segurança de senhas ao definir a senha de partições criptografadas e memorize-a também. Sem a senha, os dados criptografados não podem ser acessados nem restaurados.

A caixa de diálogo do especialista do YaST em particionamento, descrita na Seção “Particionador” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização), oferece as opções necessárias para criar uma partição criptografada. Clique em *Criar* como se estivesse criando uma partição normal. Na caixa de diálogo exibida, digite os parâmetros de particionamento para a nova partição, como a formatação desejada e o ponto de montagem. Para concluir o processo, clique em *Sistema de Arquivo Criptografado*. Na caixa de diálogo seguinte, digite a senha duas vezes. A nova partição criptografada é criada depois que você clica em *OK* para fechar a caixa de diálogo de particionamento. Durante a inicialização, o sistema operacional solicita a senha antes da montagem da partição.

Se você não quiser montar a partição criptografada durante a inicialização, clique em Enter quando a senha for solicitada. Em seguida, não digite a senha novamente. Nesse caso, o sistema de arquivos criptografado não será montado, e o sistema operacional

continuará a inicialização bloqueando o acesso aos seus dados. Uma vez montada, a partição estará disponível a todos os usuários.

Se o sistema de arquivos criptografado somente for montado quando necessário, habilite a opção *Não Montar na Inicialização do Sistema* na caixa de diálogo *Opções de fstab*. A respectiva partição não será montada durante a inicialização do sistema. Para torná-la disponível no futuro, monte-a manualmente com `mount` *`nome_da_partição ponto_de_montagem`*. Digite a senha quando solicitada. Após terminar o trabalho na partição, desmonte-a com `umount nome_da_partiç o` para protegê-la contra o acesso de outros usuários.

Criando uma partição criptografada em um sistema em execução

ATENÇÃO: Ativando a criptografia em um sistema em execução

Também é possível criar partições criptografadas em um sistema em execução como ocorre na instalação. Contudo, a criptografia de uma partição existente destrói todos os respectivos dados.

Em um sistema em execução, selecione *Sistema* → *Particionamento* no centro de controle do YaST. Clique em *Sim* para continuar. Em vez de selecionar *Criar* como mencionado acima, clique em *Editar*. O restante do procedimento é igual.

Instalando arquivos criptografados

Em vez de usar uma partição, é possível criar sistemas de arquivos criptografados dentro de arquivos individuais para armazenar dados confidenciais. Esses sistemas são criados na mesma caixa de diálogo do YaST. Selecione *Arquivo Crypt* e digite o caminho do arquivo a ser criado, bem como seu tamanho pretendido. Aceite as configurações de formatação propostas e o tipo do sistema de arquivos. Em seguida, especifique o ponto de montagem e decida se o sistema de arquivos criptografado deve ser montado quando o sistema for inicializado.

A vantagem dos arquivos criptografados é que eles podem ser adicionados sem o reparticionamento do disco rígido. Eles são montados com a ajuda de um dispositivo de loop e se comportam como partições normais.

Usando o vi para criptografar arquivos

A desvantagem de usar partições criptografadas é que, enquanto elas são montadas, pelo menos `root` pode acessar os dados. Para evitar isso, o vi pode ser usado no modo criptografado.

Use `vi -x` *`nomedoarquivo`* para editar um novo arquivo. O vi solicita que você defina uma senha e, em seguida, criptografa o conteúdo do arquivo. Sempre que você acessar esse arquivo, o vi solicitará a senha correta.

Para obter mais segurança, você pode incluir o arquivo de texto criptografado em uma partição criptografada. Isso é recomendável porque a criptografia usada no vi não é muito eficiente.

23.3.2 Criptografando o conteúdo da mídia removível

O YaST trata a mídia removível, ou seja, discos rígidos externos ou unidades flash USB, como qualquer outro disco rígido. É possível criptografar arquivos ou partições nesse tipo de mídia, como descrito acima. Contudo, não faça a montagem dessas mídias durante a inicialização do sistema, pois normalmente elas só ficam conectadas enquanto o sistema está em execução.

23.4 Segurança e confidencialidade

Uma das principais características de um sistema Linux ou UNIX é sua capacidade de manter vários usuários ao mesmo tempo (multiusuário) e permitir que esses usuários executem inúmeras tarefas (multitarefas) no mesmo computador simultaneamente. Além disso, o sistema operacional é transparente à rede. Os usuários normalmente não sabem se os dados e aplicativos que usam são fornecidos localmente por suas máquinas ou disponibilizados pela rede.

Com o recurso multiusuário, os dados de usuários diferentes precisam ser armazenados separadamente. A segurança e privacidade precisam ser garantidas. A segurança dos dados já era considerada uma questão importante, mesmo antes de os computadores poderem se vincular através de redes. Como nos dias de hoje, a maior preocupação era

a capacidade de manter os dados disponíveis, apesar da perda ou danificação do meio dos dados, na maioria das vezes, um disco rígido.

Esta seção enfoca, principalmente, problemas de confidencialidade e formas de proteger a privacidade de usuários. Porém, ela não se estende o suficiente para abordar o conceito abrangente de segurança, que deve sempre incluir procedimentos para ter um backup regularmente atualizado, utilizável e testado à disposição. Sem isso, você pode ter muita dificuldade na recuperação de seus dados—não só no caso de algum defeito de hardware, mas também se suspeitar de alguém ter adquirido acesso não autorizado e falsificado arquivos.

23.4.1 Segurança local e de rede

Há várias formas de acessar dados:

- comunicação pessoal com quem possui as informações desejadas ou acesso aos dados através de um computador
- diretamente do console de um computador (acesso físico)
- através de uma linha serial
- usando um link de rede

Em todos esses casos, o usuário deve ser autenticado antes de acessar os recursos ou dados em questão. Um servidor da Web talvez seja menos restritivo a esse respeito, ainda assim, você não gostaria que ele divulgasse todos os seus dados pessoais para qualquer pessoa na rede.

Na lista acima, o primeiro caso é onde a maior quantidade de interação humana está envolvida, por exemplo, quando você contacta um funcionário de um banco e ele solicita que você prove que é a pessoa proprietária daquela conta de banco. Então, solicitam sua assinatura, um PIN ou uma senha para provar que você é aquela pessoa. Em alguns casos, pode ser possível extrair informações de uma pessoa esclarecida apenas mencionando poucos detalhes conhecidos, suficientes para ganhar a confiança dessa pessoa, usando uma retórica inteligente. A vítima pode ser levada a revelar, gradativamente, mais informações, talvez sem nem mesmo se dar conta disso. Entre os hackers, isso é chamado de *engenharia social*. A única forma de se proteger contra isso é educar as pessoas e saber lidar com linguagem e informações de uma forma consciente. Antes de invadirem sistemas de computador, os invasores geralmente tentam atingir

recepcionistas, auxiliares que trabalham na empresa ou até mesmo membros de uma família. Em muitos casos, como um ataque baseado em engenharia social, ele só é descoberto muito tempo depois.

Uma pessoa que deseja obter acesso não autorizado aos seus dados poderia também tentar obtê-lo da forma tradicional, diretamente através do seu hardware. Portanto, a máquina deve ser protegida contra qualquer falsificação, para que ninguém possa remover, substituir ou danificar seus componentes. Isso também se aplica a backups e, até mesmo, a qualquer cabo de rede ou de energia. Proteja também o procedimento de inicialização, pois há algumas combinações de tecla bastante conhecidas que podem provocar um comportamento anormal. Proteja-se contra isso, configurando senhas para o BIOS e para o carregador de boot.

Os terminais seriais conectados a portas seriais ainda são usados em muitos locais. Diferente das interfaces de rede, eles não usam um protocolo de rede para se comunicar com o host. Um cabo simples ou porta infravermelha envia e retorna caracteres simples entre os dispositivos. O próprio cabo é o ponto mais fraco de um sistema desses: com uma impressora mais antiga conectada a ele, é fácil registrar qualquer coisa que seja transmitida pelos cabos. O que se consegue com uma impressora também pode ser feito de outras formas, dependendo do esforço envolvido no ataque.

Ler um arquivo localmente em um host exige outras regras de acesso, diferentes de abrir uma conexão de rede com um servidor em um host diferente. Não há distinção entre segurança local e segurança de rede. A linha é desenhada onde os dados devem ser colocados em pacotes para serem enviados para outro local.

Segurança local

A segurança local começa com o ambiente físico, no local onde o computador é executado. Configure sua máquina em um local onde a segurança esteja de acordo com suas expectativas e necessidades. O principal objetivo da segurança local é manter usuários separados entre si, para que nenhum assuma a permissão ou a identidade do outro. Essa é uma regra geral a ser observada, mas é extremamente verdadeira para o `root` do usuário, que contém a força suprema do sistema. `root` pode assumir a identidade de qualquer usuário local sem que lhe seja solicitada uma senha e pode ler qualquer arquivo armazenado localmente.

Senhas

Em um sistema Linux, as senhas não são armazenadas como texto simples e a string de texto digitada não corresponde diretamente com o padrão salvo. Se fosse assim, todas as contas do seu sistema estariam comprometidas assim que alguém tivesse acesso ao arquivo correspondente. Em vez disso, a senha armazenada é criptografada e, toda vez que é digitada, é novamente criptografada para que as duas strings criptografadas sejam comparadas. Isso oferece mais segurança somente se a senha criptografada não puder ser computada de forma inversa na string de texto original.

Isso pode ser feito através de um tipo especial de algoritmo, também chamado de *algoritmo trapdoor*, pois ele só funciona em uma direção. Um invasor que obteve a string criptografada não é capaz de obter sua senha simplesmente aplicando o mesmo algoritmo novamente. Em vez disso, seria preciso testar todas as combinações de caracteres possíveis, até encontrar uma que se parecesse com sua senha quando criptografada. Em senhas com oito caracteres, há um número considerável de combinações possíveis de serem calculadas.

Nos anos setenta, dizia-se que esse método seria mais seguro do que outros, devido à relativa lentidão do algoritmo usado, que levava alguns segundos para criptografar apenas uma senha. Entretanto, enquanto isso, os PCs foram se tornando mais potentes o suficiente para executar centenas de milhares ou até milhões de criptografias por segundo. Por causa disso, as senhas criptografadas não devem ficar visíveis para usuários regulares (`/etc/shadow` não pode ser lida por usuários normais). É até mais importante que senhas não sejam fáceis de adivinhar, no caso de um arquivo de senha ficar visível por algum erro. Conseqüentemente, não é de muita utilidade "traduzir" uma senha como "tantalize" para "t@nt@1lz3".

Substituir algumas letras da palavra por números parecidos não é seguro o suficiente. Programas para fraudar senhas, que usam dicionários para adivinhar palavras, também testam substituições como essa. Uma forma melhor é criar uma palavra sem um significado comum, mas que só faça sentido para você, como as primeiras letras das palavras de uma frase ou do título de um livro, como "The Name of the Rose" by Umberto Eco (O Nome da Rosa, de Umberto Eco). A senha segura criada ficaria assim: "TNotRbUE9". Diferentemente, senhas como "beerbuddy" ou "jasmine76" são de fácil adivinhação, mesmo por alguém que tenha pouco conhecimento a seu respeito.

O procedimento de inicialização

Configure o sistema de forma que não possa ser inicializado de um disquete ou CD, removendo totalmente as unidades ou configurando uma senha para o BIOS e configurando-o para que inicialize somente a partir de um disco rígido. Normalmente, um sistema Linux é iniciado por um carregador de boot, permitindo que você passe opções adicionais para o kernel inicializado. Para evitar que outros usem esses parâmetros durante a inicialização, configure uma senha adicional em `/boot/grub/menu.lst` (consulte o Capítulo 29, *O Carregador de Boot* (p 453)). Isso é imprescindível para a segurança do sistema. O kernel não só é executado com permissões de `root`, como também é a primeira autoridade a conceder permissões de `root` na inicialização do sistema.

Permissões de arquivo

Como regra geral, sempre trabalhe com os privilégios mais restritivos possíveis para uma determinada tarefa. Por exemplo, definitivamente, não é necessário ser `root` para ler ou gravar e-mails. Se o programa de correio possuir um bug, esse bug pode ser explorado para um ataque que atue com as permissões exatas do programa quando foi inicializado. Ao seguir a regra acima, os possíveis danos serão minimizados.

As permissões de mais de 200.000 arquivos incluídos em uma distribuição SUSE são escolhidos cuidadosamente. Um administrador de sistemas que instale softwares adicionais ou outros arquivos deve ser cuidadoso ao fazê-lo, especialmente quando configurar os bits de permissão. Administradores de sistemas experientes e atentos à segurança sempre usam a opção `-l` com o comando `ls`, para obter uma lista de arquivos extensa, que ajuda na detecção imediata de qualquer permissão de arquivo incorreta. Um atributo de arquivo incorreto não significa somente que os arquivos podem ser mudados ou apagados. Esses arquivos modificados podem ser executados pelo `root` ou, no caso de arquivos de configuração, programas poderiam usar tais arquivos com as permissões do `root`. Isso aumenta significativamente as possibilidades de um ataque. Ataques como esse são chamados de cuckoo eggs (ovos de cuco), pois o programa (o ovo) é executado (quebrado) por um usuário diferente (pássaro), exatamente como um cuco engana outros pássaros para quebrar seus ovos.

Um sistema SUSE Linux inclui os arquivos `permissions`, `permissions.easy`, `permissions.secure` e `permissions.paranoid`, todos no diretório `/etc`. A função desses arquivos é definir permissões especiais, como diretórios graváveis mundialmente ou, para arquivos, o bit do setuser ID (programas com o conjunto de bits

setuser ID não são executados com as permissões do usuário que os inicializou e sim com as do proprietário do arquivo, na maioria dos casos, o `root`). Um administrador pode usar o arquivo `/etc/permissions.local` para adicionar suas próprias configurações.

Para definir qual dos arquivos acima é usado pelos programas de configuração do SUSE para definir permissões compatíveis, selecione *Segurança* no YaST. Para saber mais sobre esse tópico, leia os comentários em `/etc/permissions` ou consulte a página do manual do `chmod` (`man chmod`).

Bugs de string de formato e overflows de buffer

Deve-se ter extremo cuidado sempre que um programa cuja função é processar dados possa ser modificado por um usuário. Porém, esse é um problema mais para o programador de um aplicativo do que para usuários regulares. O programador deve verificar se o aplicativo interpreta os dados de forma correta, sem gravá-lo em áreas da memória muito pequenas para mantê-lo. Da mesma forma, o programa deve manter os dados de forma consistente, usando as interfaces definidas para esse fim.

Um *overflow de buffer* pode ocorrer se o tamanho real do buffer da memória não for levado em conta quando uma gravação for feita nesse buffer. Há casos em que esses dados (como os gerados pelo usuário) usam mais espaço do que o disponibilizado no buffer. Como conseqüência, os dados são gravados além da área final do buffer, o que, em certas circunstâncias, possibilita que um programa execute seqüências de programa influenciado pelo usuário (e não pelo programador), em vez de apenas processar os dados do usuário. Um bug desse tipo pode trazer sérias conseqüências, especialmente se o programa estiver sendo executado com privilégios especiais (consulte a “Permissões de arquivo” (p 355)).

Bugs de string de formato funciona um pouco diferente, porém novamente é a entrada do usuário que pode controlar a bandeja do programa. Na maioria dos casos, esses erros de programação são explorados com programas executados com permissões especiais—programas setuid e setgid—o que também significa que você pode proteger os dados e o sistema desses bugs, removendo dos programas os privilégios de execução correspondentes. Novamente, a melhor forma é aplicar uma política de uso de privilégios mais baixos possíveis (consulte a “Permissões de arquivo” (p 355)).

Como os overflows de buffer e bugs de string de formato são bugs relacionados ao manuseio de dados do usuário, eles não são só exploráveis se o acesso tiver sido concedido a uma conta local. Muitos dos bugs relatados também podem ser explorados

por um link de rede. Da mesma forma, bugs de string de formato e overflows de buffer devem ser classificados como relevantes tanto para a segurança de rede quanto a local.

Vírus

Contrário ao que dizem algumas pessoas, há vírus que são executados no Linux. Entretanto, os vírus conhecidos foram criados por seus autores como um *protótipo*, para provar que a técnica funciona como determinado. Nenhum desses vírus foi apontado *em lugar algum* até agora.

Os vírus não conseguem sobreviver e se espalharem sem que haja um host onde possam permanecer. Nesse caso, o host seria um programa ou uma área de armazenamento importante do sistema, como o MBR (Master Boot Record), que precisa ser gravável para o código de programa do vírus. Devido aos seus recursos de multiusuário, o Linux pode restringir o acesso de gravação a certos arquivos especialmente importantes para arquivos do sistema. Portanto, se você trabalhou normalmente com as permissões de `root`, as chances de o sistema ser infectado por vírus aumentarão. Por outro lado, se você seguiu os princípios do uso de privilégios mais baixos possíveis, conforme mencionado anteriormente, há poucas chances de um vírus entrar no computador.

Independente disso, nunca execute um programa às pressas a partir de algum site da Internet que você não conheça bem. Os pacotes RPM do SUSE possuem uma assinatura criptográfica como rótulo digital indicando o extremo cuidado utilizado durante sua criação. Os vírus são um sinal típico de que o administrador ou o usuário não possuem uma precaução de segurança necessária, colocando em risco um sistema que deveria estar altamente protegido.

Vírus não devem ser confundidos com worms, que pertencem inteiramente ao mundo das redes. Worms não precisam de um host para se espalharem.

Segurança de rede

A segurança da rede é importante para a proteção contra um ataque iniciado externamente. O procedimento de login típico, que exige um nome de usuário e senha para a autenticação do usuário ainda é uma questão de segurança local. No caso específico de efetuar login em uma rede, existe uma diferença entre os dois aspectos de segurança. O que acontece até a autenticação real é a segurança da rede e tudo o que acontece depois disso é a segurança local.

Sistema x window e autenticação x

Conforme mencionado no início, a transparência da rede é uma das características principais de um sistema UNIX. X, o sistema de janelas dos sistemas operacionais do UNIX, usa esse recurso de uma forma impressionante. Com X, basicamente não há problemas para efetuar login em um host remoto e iniciar um programa gráfico que será, depois, enviado para a rede para ser exibido no computador.

Quando um cliente X deve ser exibido remotamente usando um servidor X, o último deve proteger o recurso gerenciado por ele (a tela) de acessos não autorizados. Em termos mais concretos, certas permissões precisam ser fornecidas ao programa cliente. Com o sistema X Window, há duas formas de fazer isso, chamadas controle de acesso baseado em host e controle de acesso baseado em cookie. O anterior se baseia no endereço IP do host onde o cliente deve ser executado. O programa que controla isso é o xhost. O xhost. insere o endereço IP de um cliente legítimo em um banco de dados mínimo pertencente ao servidor X. Entretanto, basear-se em endereços IP para autenticação não é muito seguro. Por exemplo, se houvesse um segundo usuário trabalhando no host que envia o programa cliente, esse usuário também teria acesso ao servidor X—o mesmo acesso de alguém que desejasse roubar o endereço IP. Devido a essas faltas, esse método de autenticação não é descrito mais detalhadamente aqui, mas você pode obter mais informações sobre ele com o `man xhost`.

No caso do controle de acesso baseado em cookie, uma string de caracteres gerada é conhecida somente pelo servidor X e pelo usuário legítimo, da mesma forma que uma placa ID de algum tipo. Esse cookie (a palavra é originada não de cookies (biscoitos) comuns, mas dos fortune cookies chineses (biscoitos da sorte chineses) que contêm um epigrama) é armazenado durante o login no arquivo `.Xauthority` no diretório principal do usuário e fica disponível para qualquer cliente X que deseje usar o servidor X para exibir uma janela. O arquivo `.Xauthority` pode ser examinado pelo usuário com a ferramenta xauth. Se você renomeasse o `.Xauthority` ou se apagasse acidentalmente o arquivo do seu diretório principal, não conseguiria abrir nenhuma janela ou cliente X novos. Leia mais sobre os mecanismos de segurança do sistema X Window na página do manual do Xsecurity (`man Xsecurity`).

O SSH (secure shell) pode ser usado para criptografar uma conexão de rede completamente e encaminhá-la para um servidor X de forma transparente, sem que o mecanismo de criptografia seja percebido pelo usuário. Também é chamado de encaminhamento de X. O encaminhamento de X é feito simulando um servidor X no lado do servidor e configurando uma variável DISPLAY para o shell no host remoto.

Informações detalhadas sobre o SSH podem ser encontradas em Seção 23.2, “SSH: operações seguras de rede” (p 342).

ATENÇÃO

Se você não considera seguro o host onde efetua login, não use o encaminhamento de X. Com o encaminhamento de X habilitado, um invasor pode se autenticar através da conexão SSH e invadir o servidor X para farejar sua entrada de teclado, por exemplo.

Bugs de string de formato e overflows de buffer

Conforme discutido na “Bugs de string de formato e overflows de buffer” (p 356), os bugs de overflows de buffer e de strings de formato devem ser classificados como relevantes tanto para a segurança de rede quanto a local. Como as variantes locais desses bugs, os overflows de buffer em programas de rede, quando são explorados com sucesso, quase sempre são usados para obter permissões de `root`. Mesmo que não seja o caso, um invasor poderia usar o bug para ter acesso a uma conta local não privilegiada para explorar quaisquer outras vulnerabilidades que pudessem existir no sistema.

Bugs de overflows de buffer e de strings de formato exploráveis em um link de rede são, certamente, a forma mais freqüente de ataques remotos em geral. As explorações desses programas—que exploram furos de segurança recentemente encontrados—geralmente são enviadas para listas de discussão de segurança. Elas podem ser usadas para identificar a vulnerabilidade, sem saber os detalhes do código. Através dos anos, a experiência mostrou que a disponibilidade de códigos de exploração contribuiu para a criação de sistemas operacionais mais seguros, obviamente devido ao fato de os criadores de sistemas operacionais terem sido forçados a consertar os problemas em seus softwares. Com software livre, qualquer pessoa tem acesso ao código fonte (o SUSE Linux vem com todos os códigos fonte disponíveis) e qualquer um que encontre uma vulnerabilidade e seu código de exploração poderá submeter um patch para consertar o bug correspondente.

DoS (Denial of Service)

A finalidade de um ataque DoS (denial of service) é bloquear um programa de servidor ou mesmo todo o sistema, algo que pode ser realizado de várias formas: sobrecarregar o servidor, mantendo-o ocupado com pacotes de lixo ou explorar um overflow de buffer remoto. Geralmente, a única finalidade de um ataque DoS é fazer o serviço desaparecer.

Entretanto, quando um determinado serviço não está mais disponível, as comunicações podem ficar vulneráveis a *ataques man-in-the-middle* (farejamento, roubo de conexão de TCP, falsificação) e envenenamento do DNS.

Man in the middle: farejamento, roubo, falsificação

Em geral, qualquer ataque remoto executado por um invasor que se coloca entre os hosts de comunicação é chamado de *ataque man-in-the-middle*. O que a maioria dos tipos de ataques man-in-the-middle tem em comum é que a vítima, geralmente, não percebe o que está acontecendo. Há muitas variantes possíveis, por exemplo, o invasor pode escolher uma solicitação de conexão e encaminhá-la para a máquina de destino. Agora, a vítima estabeleceu, involuntariamente, uma conexão com o host errado, porque a outra extremidade está posando como a máquina de destino legítima.

A forma mais simples de um ataque man-in-the-middle se chama *sniffer*—o invasor "apenas" escuta a passagem do tráfego de rede. Em um ataque mais complexo, o "man in the middle" pode tentar controlar uma conexão já estabelecida (roubar). Para fazer isso, o invasor precisa analisar os pacotes durante algum tempo, para ser capaz de prever os números da seqüência do TCP pertencentes à conexão. Quando o invasor finalmente identifica a função do host de destino, as vítimas percebem isso, pois elas recebem uma mensagem de erro informando que a conexão foi encerrada devido a uma falha. O que facilita os invasores é o fato de haver protocolos pouco seguros contra roubos através de criptografia, que apenas executam um procedimento de autenticação simples quando estabelecem a conexão.

Falsificação é um ataque onde os pacotes são modificados para conter dados de origem falsificada, normalmente, o endereço IP. A maioria dos ataques ativos se baseia em enviar esses pacotes falsos—algo que, em uma máquina Linux, só pode ser feito pelo superusuário (`root`).

Muitos dos ataques mencionados são executados junto com um DoS. Se um invasor vir uma oportunidade de desativar abruptamente um host, mesmo que por um curto período, será mais fácil para ele usar o ataque ativo, pois o host não será capaz de interferir contra o ataque por algum tempo.

Envenenamento de DNS

O envenenamento de DNS significa que o invasor corrompe o cache de um servidor DNS respondendo a ele com pacotes de respostas de DNS falsificados, para tentar fazer

com que o servidor envie certos dados a uma vítima que esteja solicitando informações a esse servidor. Muitos servidores mantêm uma relação de confiança com outros hosts, baseada nos endereços IP ou nos nomes de host. O invasor precisa ter um bom conhecimento da estrutura real das relações de confiança entre os hosts, para ser distinguido como um dos hosts confiáveis. Normalmente, o invasor analisa alguns pacotes recebidos do servidor para obter as informações necessárias. O invasor geralmente também precisa planejar um ataque DoS bem programado ao servidor de nomes. Proteja-se, usando conexões criptografadas que possam verificar a identidade dos hosts aos quais deve se conectar.

Worms

Worms geralmente são confundidas com vírus, mas há uma clara diferença entre os dois. Diferente dos vírus, worms não precisam infectar um programa de host para viverem. Em vez disso, suas especialidades são se espalharem o mais rápido possível por estruturas de rede. Os worms que apareciam antigamente, como Ramen, Lion ou Adore, faziam uso de falhas conhecidas na segurança dos programas de servidor, como bind8 ou lprNG. A proteção contra worms é relativamente fácil. Considerando que um certo tempo decorre entre a descoberta de uma falha na segurança e o momento em que o worm entra no servidor, há uma boa chance de uma versão atualizada do programa afetado estar disponível a tempo. Isso só tem utilidade se o administrador realmente instalar as atualizações de segurança nos sistemas em questão.

23.4.2 Algumas dicas e truques gerais de segurança

Para usar a segurança de forma competente, é importante estar atualizado com os novos produtos desenvolvidos e manter-se informado sobre as questões de segurança mais recentes. Uma boa forma de proteger o sistema contra problemas de todos os tipos é obter e instalar os pacotes atualizados recomendados pelos anúncios de segurança o mais rápido possível. Os anúncios de segurança do SUSE são publicados em uma lista de discussão na qual você pode se inscrever através do link `http://www.novell.com/linux/security/securitysupport.html`. A lista `suse-security-announce@suse.de` é a fonte principal de informações referente a pacotes atualizados e inclui membros da equipe de segurança do SUSE entre seus contribuintes ativos.

A lista de discussão suse-security@suse.de é um bom local para discutir quaisquer problemas de segurança de seu interesse. Inscreva-se nela na mesma página da Web.

bugtraq@securityfocus.com é uma das listas de discussão sobre segurança mais conhecidas no mundo. A leitura dessa lista, que recebe entre 15 a 20 publicações por dia, é recomendada. Mais informações podem ser encontradas em http://www.securityfocus.com.

A seguir, uma lista de regras que podem ser úteis para lidar com questões de segurança básica:

- De acordo com a regra de uso do conjunto de permissões mais restritivo para cada trabalho, evite fazer seus trabalho regulares no `root`. Isso reduzirá o risco de obter um cuckoo egg (ovo do cuco) ou um vírus e protegerá seu computador dos seus próprios erros.

- Se possível, tente sempre usar conexões criptografadas para trabalhar em uma máquina remota. O uso de `ssh` (shell seguro) para substituir `telnet`, `ftp`, `rsh` e `rlogin` deve ser uma prática padrão.

- Evite usar métodos de autenticação baseados em endereços IP isolados.

- Tente manter os pacotes relacionados à rede mais importantes atualizados e inscreva-se nas listas de discussão correspondentes, para receber anúncios sobre novas versões desses programas (bind, sendmail, ssh, etc.). O mesmo deve se aplicar aos softwares relevantes à segurança local.

- Mude o arquivo `/etc/permissions`, para otimizar as permissões dos arquivos cruciais para a segurança do seu sistema. Se você remover o setuid bit de um programa, haverá grandes chances de ele não ser mais capaz de executar suas respectivas funções da forma devida. Por outro lado, considere que, na maioria dos casos, o programa não será mais um risco potencial à segurança. Você pode usar um método semelhante, com arquivos e diretórios internacionalmente graváveis.

- Desabilite quaisquer serviços de rede que não sejam absolutamente necessários para o servidor funcionar adequadamente. Isso torna o sistema mais seguro. Portas abertas, com o estado do socket LISTEN, podem ser encontradas no programa netstat. Para as opções, é recomendável usar `netstat -ap` ou `netstat -anp`. A opção `-p` permite que você veja que processo está ocupando uma porta com qual nome.

Compare os resultados do netstat com os de uma exploração de porta mais completa feita fora do host. Um programa excelente para esse trabalho é o nmap, que não só verifica as portas da máquina, como também conclui quais serviços estão aguardando atrás delas. Entretanto, a exploração da porta pode ser interpretada como um ato agressivo, portanto, não a faça em um host sem a aprovação explícita do administrador. Por fim, lembre-se de que é importante não só explorar as portas TCP, mas também as portas UDP (opções `-sS` e `-sU`).

- Para monitorar a integridade dos arquivos do seu sistema de forma confiável, use o programa AIDE (Advanced Intrusion Detection Environment), disponível no SUSE Linux. Criptografe o banco de dados criado pelo AIDE, para evitar que alguém o falsifique. Além disso, mantenha um backup desse banco de dados disponível fora da máquina, armazenado em um meio de dados externo não conectado à rede.

- Instale cuidadosamente qualquer software de terceiros. Houve casos de um hacker ter criado um Cavalo de Tróia no arquivo tar de um pacote de softwares de segurança, mas, felizmente, o ataque foi descoberto rapidamente. Se você instalar um pacote binário, não tenha dúvidas quanto ao site de onde foi feito o seu download.

  Os pacotes RPM do SUSE são gpg-signed (assinados pelo gpg). A chave usada pelo SUSE para a assinatura é:

  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>

  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

  O comando `rpm --checksig package.rpm` mostra se o checksum e a assinatura de um pacote desinstalado estão corretos. Encontre a chave no primeiro CD de distribuição e na maioria dos servidores de chaves em todo o mundo.

- Verifique os backups de arquivos do sistema e usuário regularmente. Considere que, se você não testar os backups para ver se funcionam, eles serão, na verdade, inúteis.

- Verifique seus arquivos de registro. Sempre que possível, grave um pequeno script para pesquisar entradas suspeitas. Com certeza, essa não é exatamente uma tarefa trivial. No final, somente você saberá quais entradas não são comuns e quais são.

- Use o `tcp_wrapper` para restringir o acesso a serviços individuais executados na sua máquina, para que você tenha controle total sobre quais endereços IP podem se conectar a um serviço. Para obter informações adicionais referentes ao `tcp_wrapper`, consulte as páginas do manual do tcpd e do hosts_access (`man 8 tcpd`, `man hosts_access`).
- Use o SuSEfirewall para aprimorar a segurança fornecida pelo tcpd (tcp_wrapper).
- Defina suas medidas de segurança para serem redundantes: uma mensagem vista duas vezes é melhor do que não ver mensagem alguma.

23.4.3 Usando o Central Security Reporting Address (Endereço de Relatórios de Segurança Central)

Se encontrar um problema relacionado à segurança (verifique, primeiro, os pacotes de atualização disponíveis), escreva um e-mail para `security@suse.de`. Inclua uma descrição detalhada do problema e o número de versão do pacote em questão. O SUSE tentará enviar uma resposta o mais rápido possível. Você é incentivado a criptografar por pgp suas mensagens de e-mail. A chave pgp do SUSE é:

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Essa chave também está disponível para download em `http://www.novell.com/linux/security/securitysupport.html`.

Listas de controle de acesso no Linux

24

Este capítulo apresenta um breve resumo do segundo plano e das funções das ACLs (listas de controle de acesso) POSIX para os sistemas de arquivos do Linux. As ACLs podem ser usadas como expansão do conceito tradicional de permissão para objetos do sistema de arquivos. Com as ACLs, as permissões podem ser definidas com mais flexibilidade do que permite o conceito de permissão tradicional.

O termo *ACL POSIX* sugere que este é um verdadeiro padrão POSIX (*portable operating system interface*). Os respectivos padrões de rascunho POSIX 1003.1e e POSIX 1003.2c foram removidos por vários motivos. Contudo, as ACLs, como encontradas em vários sistemas pertencentes à família UNIX, são baseadas nesses rascunhos, e a implementação das ACLs do sistema de arquivos, como descrita neste capítulo, também segue esses padrões. Elas podem ser vistas em `http://wt.xpilot.org/publications/posix.1e/`.

24.1 Vantagens das ACLs

Tradicionalmente, três conjuntos de permissões são definidos para cada objeto de arquivo em um sistema Linux. Esses conjuntos incluem as permissões de leitura (`r`), gravação (`w`) e execução (`x`) para cada um dos três tipos de usuários: o proprietário do arquivo, o grupo e os outros usuários. Além disso, é possível definir o *set user id*, o *set group id* e o *sticky* bit. Este conceito simples é completamente adequado para a maioria dos casos práticos. Porém, para os cenários mais complexos ou aplicativos avançados, os administradores de sistema tiveram que usar anteriormente várias estratégias para se esquivar das limitações do conceito tradicional de permissão.

As ACLs podem ser usadas em situações que exigem uma extensão do conceito tradicional de permissão de arquivo. Elas admitem a atribuição de permissões a usuários individuais ou a grupos, mesmo que eles não correspondam ao proprietário original ou ao grupo proprietário. As listas de controle de acesso são um recurso do kernel do Linux e são atualmente suportadas por ReiserFS, Ext2, Ext3, JFS e XFS. Com as ACLs, cenários complexos podem ser realizados sem a implementação de modelos de permissão complexos no nível do aplicativo.

As vantagens das ACLs ficam muito evidentes em situações como a substituição de um servidor Windows por um servidor Linux. Algumas das estações de trabalho conectadas podem continuar em execução no Windows, mesmo após a migração. O sistema Linux oferece serviços de arquivo e impressão para os clientes Windows com Samba. Levando-se em consideração que o Samba suporta listas de controle de acesso, as permissões de usuário podem ser configuradas em servidores Linux e Windows com interface gráfica do usuário (somente Windows NT e posterior). Com o winbindd, é possível até mesmo atribuir permissões a usuários que existem somente no domínio do Windows sem nenhuma conta no servidor Linux.

24.2 Definições

classe de usuário
O conceito convencional de permissão POSIX utiliza três *classes* de usuários para atribuir permissões no sistema de arquivos: o proprietário, o grupo proprietário e os outros usuários. Três bits de permissões podem ser definidos para cada classe de usuário, concedendo permissão de leitura (`r`), gravação (`w`) e execução (`x`).

ACL de acesso
As permissões de acesso de usuário e grupo para todos os tipos de objetos Sistema de arquivos (arquivos e diretórios) são determinadas através das ACLs de acesso.

ACL padrão

As ACLs padrão podem ser aplicadas somente a diretórios. Elas determinam as permissões que um objeto Sistema de arquivos herda de seu diretório pai quando é criado.

entrada de ACL
Cada ACL consiste em um conjunto de entradas de ACL. Uma entrada de ACL contém um tipo (consulte a Tabela 24.1, “Tipos de entrada de ACL” (p 368)), um

qualificador para o usuário ou o grupo ao qual a entrada se refere e um conjunto de permissões. Para alguns tipos de entrada, o qualificador para o grupo ou usuários é indefinido.

24.3 Gerenciando ACLs

A Tabela 24.1, “Tipos de entrada de ACL” (p 368) resume os seis tipos possíveis de entradas de ACL, cada um definindo permissões para um usuário ou um grupo de usuários. A entrada *proprietário* define as permissões do usuário proprietário do arquivo ou diretório. A entrada *grupo proprietário* define as permissões do grupo proprietário do arquivo. O superusuário pode mudar o proprietário ou o grupo proprietário com `chown` ou `chgrp`. Neste caso, as entradas de proprietário e grupo proprietário referem-se ao novo usuário e grupo proprietário. Cada entrada de *usuário nomeado* define as permissões do usuário especificado no campo qualificador da entrada, que é o campo do meio no formulário de texto exibido na Tabela 24.1, “Tipos de entrada de ACL” (p 368). Cada entrada *grupo nomeado* define as permissões do grupo especificado no campo qualificador da entrada. Somente as entradas usuário nomeado e grupo nomeado possuem um campo qualificador que não está vazio. A entrada *outros* define as permissões de todos os outros usuários.

A entrada *máscara* limita ainda mais as permissões concedidas pelas entradas *usuário nomeado*, *grupo nomeado* e *grupo proprietário* ao definir qual das permissões naquelas entradas são efetivas e quais são mascaradas. Se existirem permissões em uma das entradas mencionadas, assim como na máscara, elas serão efetivas. As permissões contidas somente na máscara ou somente na entrada real não são efetivas, significando que as permissões não são concedidas. Todas as permissões definidas nas entradas *proprietário* e *grupo proprietário* são sempre efetivas. O exemplo na Tabela 24.2, “Mascarando permissões de acesso” (p 368) demonstra este mecanismo.

Existem duas classes básicas de ACLs. Uma ACL *mínima* contém somente as entradas dos tipos *proprietário*, *grupo proprietário* e *outros*, que correspondem aos bits de permissão convencionais para arquivos e diretórios. Uma ACL *estendida* vai além disso. Ela deve conter uma entrada *máscara* e pode conter várias entradas dos tipos *usuário nomeado* e *grupo nomeado*.

Tabela 24.1 *Tipos de entrada de ACL*

Tipo	Formato do texto
proprietário	`user::rwx`
usuário nomeado	`user:name:rwx`
grupo proprietário	`group::rwx`
grupo nomeado	`group:name:rwx`
máscara	`mask::rwx`
outros	`other::rwx`

Tabela 24.2 *Mascarando permissões de acesso*

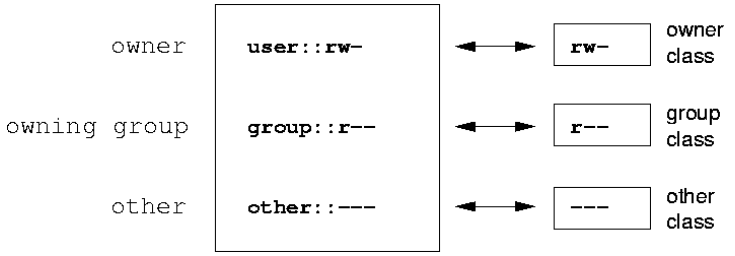
Tipo de entrada	Formato do texto	Permissões
usuário nomeado	`user:geeko:r-x`	`r-x`
máscara	`mask::rw-`	`rw-`
	permissões efetivas:	`r--`

24.3.1 Entradas de ACL e bits de permissão do modo do arquivo

A Figura 24.1, “ACL mínima: entradas de ACL comparadas a bits de permissão” (p 369) e a Figura 24.2, “ACL estendida: entradas de ACL comparadas a bits de permissão” (p 369) ilustram os dois casos de uma ACL mínima e de uma ACL estendida. As figuras são estruturadas em três blocos: o bloco esquerdo mostra as especificações de tipo das entradas de ACL, o bloco central mostra uma ACL de exemplo e o bloco direito mostra os respectivos bits de permissão, de acordo com o conceito convencional de permissão, por exemplo, como mostrado pelo comando `ls -l`. Em ambos os casos, as permissões *classe proprietária* são mapeadas para a entrada de ACL *proprietário*. As permissões

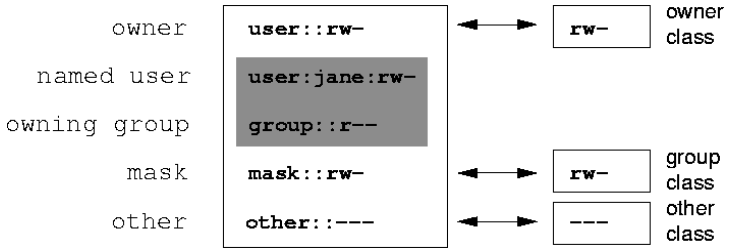
outra classe são mapeadas para a respectiva entrada de ACL. Porém, o mapeamento das permissões *classe de grupo* é diferente nos dois casos.

Figura 24.1 *ACL mínima: entradas de ACL comparadas a bits de permissão*



No caso de uma ACL mínima (sem *máscara*), as permissões *classe de grupo* são mapeadas para a entrada de ACL *grupo proprietário*. Você pode ver isso na Figura 24.1, “ACL mínima: entradas de ACL comparadas a bits de permissão” (p 369). No caso de uma ACL estendida (com *máscara*), as permissões *classe de grupo* são mapeadas para a entrada *máscara*. Você pode ver isso na Figura 24.2, “ACL estendida: entradas de ACL comparadas a bits de permissão” (p 369).

Figura 24.2 *ACL estendida: entradas de ACL comparadas a bits de permissão*



Este método de mapeamento assegura uma interação uniforme de aplicativos, tenham eles suporte a ACL ou não. As permissões de acesso que foram atribuídas através de bits de permissão representam o limite superior para todos os outros “ajustes finos” feitos com uma ACL. As mudanças feitas nos bits de permissão são refletidas pela ACL e vice-versa.

24.3.2 Diretório com uma ACL de acesso

O gerenciamento de ACLs de acesso é demonstrado no exemplo a seguir:

Antes de criar o diretório, use o comando `umask` para definir quais permissões de acesso devem ser mascaradas cada vez que um objeto de arquivo for criado. O comando `umask 027` define as permissões ao conceder ao proprietário todas as permissões (`0`), ao negar o acesso de gravação de grupo (`2`) e ao não conceder nenhuma permissão aos outros usuários (`7`). O comando `umask`, na verdade, mascara os bits de permissão correspondentes ou os desativa. Para obter detalhes, consulte a página de manual correspondente (`man umask`).

O comando `mkdir meudir` deve criar o diretório `meudir` com as permissões padrão, como definido por `umask`. Use `ls -dl meudir` para verificar se todas as permissões foram atribuídas corretamente. A saída para este exemplo é:

```
drwxr-x--- ... tux project3 ... meudir
```

Com o comando `getfacl meudir`, verifique o estado inicial da ACL. Ele fornece informações como:

```
# file: meudir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

A saída de `getfacl` reflete precisamente o mapeamento de bits de permissão e entradas ACL, como descrito na Seção 24.3.1, “Entradas de ACL e bits de permissão do modo do arquivo” (p 368). As primeiras três linhas de saída mostram o nome, o proprietário e o grupo proprietário do diretório. As próximas três linhas contêm as três entradas de ACL *proprietário*, *grupo proprietário* e *outros*. Na verdade, no caso desta ACL mínima, o comando `getfacl` não produz nenhuma informação que você não pudesse obter com o comando `ls`.

Modifique a ACL para atribuir permissões de leitura, gravação e execução para um usuário `geeko` adicional e um grupo `mascotes` com:

```
setfacl -m user:geeko:rwx,group:mascotes:rwx meudir
```

A opção `-m` solicita que `setfacl` modifique a ACL existente. O argumento a seguir indica as entradas de ACL a serem modificadas (várias entradas são separadas por vírgulas). A parte final especifica o nome do diretório no qual essas modificações devem ser aplicadas. Use o comando `getfacl` para dar uma olhada na ACL resultante.

```
# file: meudir
# owner: tux
# group: project3
```

```
user::rwx
user:geeko:rwx
group::r-x
group:mascotes:rwx
mask::rwx
other::---
```

Além das entradas iniciadas para o usuário `geeko` e o grupo `mascotes`, uma entrada *máscara* foi gerada. Esta entrada *máscara* é definida automaticamente para que todas as permissões sejam efetivas. O comando `setfacl` adapta automaticamente as entradas *máscara* existentes às configurações modificadas, a não ser que você desative este recurso com `-n`. *máscara* define as permissões máximas de acesso efetivo para todas as entradas na *classe de grupo*. Isto inclui *usuário nomeado*, *grupo nomeado* e *grupo proprietário*. Os bits de permissão de *classe de grupo* exibidos pelo comando `ls -dl meudir` agora correspondem à entrada `m scara`.

```
drwxrwx---+ ... tux project3 ... mydir
```

A primeira coluna da saída agora contém um sinal de + extra para indicar que existe uma ACL *estendida* para esse item.

De acordo com a saída do comando `ls`, as permissões para a entrada *máscara* incluem o acesso de gravação. Tradicionalmente, tais bits de permissão significariam que o *grupo proprietário* (aqui, `project3`) também teria acesso de gravação no diretório `meudir`. Porém, as permissões de acesso efetivas para o *grupo proprietário* correspondem à parte sobreposta das permissões definidas para o *grupo proprietário* e para a *máscara*, que é `r-x` em nosso exemplo (consulte a Tabela 24.2, “Mascarando permissões de acesso” (p 368)). Em relação às permissões efetivas do *grupo proprietário* neste exemplo, nada mudou mesmo após a adição das entradas de ACL.

Edite a entrada *máscara* com `setfacl` ou `chmod`. Por exemplo, use `chmod g-w meudir`. O comando `ls -dl meudir` mostrará:

```
drwxr-x---+ ... tux project3 ... meudir
```

`getfacl meudir` fornece a seguinte saída:

```
# file: meudir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascotes:rwx      # effective: r-x
mask::r-x
other::---
```

Após executar o comando `chmod` para remover a permissão de gravação dos bits *classe de grupo*, a saída do comando `ls` será suficiente para ver que os bits *máscara* devem ter mudado de acordo: a permissão de gravação é novamente limitada ao proprietário de `meudir`. A saída de `getfacl` confirma isso. Esta saída inclui um comentário para todas aquelas entradas nas quais os bits de permissão efetiva não correspondem às permissões originais, já que são filtrados de acordo com a entrada *máscara*. As permissões originais podem ser restauradas a qualquer momento com `chmod g+w meudir`.

24.3.3 Diretório com uma ACL padrão

Os diretórios podem ter uma ACL padrão, que é um tipo especial de ACL que define permissões de acesso herdadas pelos objetos no diretório quando são criados. Uma ACL padrão afeta subdiretórios e arquivos.

Efeitos em uma ACL padrão

Existem dois modos diferentes de passar as permissões de uma ACL padrão do diretório para os seus arquivos e subdiretórios:

- Um subdiretório herda a ACL padrão do diretório pai como sua ACL padrão e como uma ACL de acesso.
- Um arquivo herda a ACL padrão como a sua ACL de acesso.

Todas as chamadas de sistema que criam objetos Sistema de arquivos utilizam um parâmetro `mode` que define as permissões de acesso para o objeto Sistema de arquivos recém-criado. Se o diretório pai não tiver uma ACL padrão, os bits de permissão, como definidos por `umask`, serão subtraídos das permissões quando passados pelo parâmetro `mode`, e o resultado será atribuído ao novo objeto. Se existir uma ACL padrão para o diretório pai, os bits de permissão atribuídos ao novo objeto corresponderão à parte sobreposta das permissões do parâmetro `mode` e daqueles definidos na ACL padrão. O comando `umask` é desconsiderado neste caso.

Aplicação das ACLs padrão

Os três exemplos a seguir mostram as operações principais de diretórios e ACLs padrão:

1. Adicione uma ACL padrão ao diretório `meudir` existente com:

```
setfacl -d -m group:mascotes:r-x meudir
```

A opção `-d` do comando `setfacl` solicita que `setfacl` realize as seguintes modificações (opção `-m`) na ACL padrão.

Preste bem atenção no resultado deste comando:

```
getfacl meudir

# file: meudir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascotes:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:mascotes:r-x
default:mask::r-x
default:other::---
```

`getfacl` retorna a ACL de acesso e a ACL padrão. A ACL padrão é formada por todas as linhas que começam com `default`. Embora você tenha simplesmente executado o comando `setfacl` com uma entrada para o grupo `mascotes` na ACL padrão, `setfacl` copiou automaticamente todas as outras entradas da ACL de acesso para criar uma ACL padrão válida. As ACLs padrão não têm efeito imediato nas permissões de acesso. Elas apenas surgem quando os objetos Sistema de arquivos são criados. Esses novos objetos herdam permissões somente da ACL padrão de seu diretório pai.

2. No próximo exemplo, use `mkdir` para criar um subdiretório em `meudir`, que herda a ACL padrão.

```
mkdir meudir/meusubdir

getfacl meudir/meusubdir

# file: meudir/meusubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascotes:r-x
mask::r-x
```

```
other::---
default:user::rwx
default:group::r-x
default:group:mascotes:r-x
default:mask::r-x
default:other::---
```

Como esperado, o subdiretório `meusubdir` recém-criado tem permissões da ACL padrão do diretório pai. A ACL de acesso de `meusubdir` é um reflexo exato da ACL padrão de `meudir`. A ACL padrão que este diretório transmitirá para os seus objetos subordinados também é a mesma.

3. Use o comando `touch` para criar um arquivo no diretório `meudir`, por exemplo, `touch meudir/meuarq`. O comando `ls -l meudir/meuarq` mostrará:

```
-rw-r-----+ ... tux project3 ... meudir/meuarq
```

O resultado de `getfacl meudir/meuarq` será:

```
# file: meudir/meuarq
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascotes:r-x   # effective:r--
mask::r--
other::---
```

`touch` usa um `mode` com o valor `0666` quando cria novos arquivos, o que significa que os arquivos são criados com permissões de leitura e gravação para todas as classes de usuários, desde que não existam outras restrições em `umask` ou na ACL padrão (consulte a "Efeitos em uma ACL padrão" (p 372)). Na verdade, isto significa que todas as permissões de acesso não contidas no valor `mode` são removidas de suas respectivas entradas de ACL. Embora nenhuma permissão tenha sido removida da entrada de ACL da *classe de grupo*, a entrada *máscara* foi modificada para mascarar permissões não definidas em `mode`.

Este método assegura uma interação uniforme de aplicativos, como compiladores, com as ACLs. Você pode criar arquivos com permissões de acesso restritas e marcá-los como executáveis. O mecanismo `mask` garante que os usuários e grupos corretos poderão executá-los como desejado.

24.3.4 Algoritmo de verificação da ACL

Um algoritmo de verificação é aplicado antes que qualquer processo ou aplicativo receba acesso a um objeto Sistema de arquivos protegido por ACL. Como regra básica, as entradas de ACL são examinadas na seguinte seqüência: *proprietário*, *usuário nomeado*, *grupo proprietário* ou *grupo nomeado* e *outros*. O acesso é gerenciado de acordo com a entrada que melhor se adequar ao processo. Permissões não são cumulativas.

A situação será mais complicada se um processo pertencer a mais de um grupo e potencialmente se adaptar a várias entradas de *grupo*. Uma entrada é selecionada aleatoriamente das entradas adequadas com as permissões necessárias. Não importa qual das entradas aciona o resultado final "acesso concedido". Do mesmo modo, se nenhuma das entradas adequadas de *grupo* contiver as permissões necessárias, uma entrada selecionada aleatoriamente acionará o resultado final "acesso negado".

24.4 Suporte a ACL em aplicativos

As ACLs podem ser usadas para implementar cenários de permissão complexos que satisfaçam os requisitos dos aplicativos modernos. O conceito tradicional de permissão e as ACLs podem ser combinados de maneira inteligente. Os comandos de arquivo básicos (`cp`, `mv`, `ls` etc.) suportam ACLs, assim como o Samba.

Infelizmente, muitos editores e gerenciadores de arquivos ainda não possuem suporte a ACL. Quando se copia arquivos com o Konqueror, por exemplo, as ACLs desses arquivos são perdidas. Quando se modifica arquivos com um editor, as ACLs dos arquivos às vezes são mantidas, outras vezes não, dependendo do modo de backup do editor usado. Se o editor gravar as mudanças no arquivo original, a ACL de acesso será mantida. Se o editor gravar o conteúdo atualizado em um novo arquivo renomeado posteriormente com o antigo nome de arquivo, as ACLs poderão ser perdidas, a não ser que o editor suporte as ACLs. Não existe atualmente nenhum aplicativo de backup que mantenha ACLs, exceto o star archiver.

24.5 Para obter mais informações

Informações detalhadas sobre as ACLs estão disponíveis em `http://acl.bestbits.at/`. Consulte também as páginas de manual de `getfacl(1)`, `acl(5)` e `setfacl(1)`.

Utilitários de monitoramento do sistema

25

Vários programas e mecanismos, alguns dos quais apresentamos aqui, podem ser usados para examinar o status do sistema. Também são descritos alguns utilitários para o trabalho de rotina, bem como seus parâmetros mais importantes.

Para cada comando apresentado, são fornecidos exemplos das saídas relevantes. Nesses exemplos, a primeira linha é o comando propriamente dito (após o sinal de cifrão). Os comentários são indicados entre colchetes (`[...]`) e linhas extensas são reduzidas quando necessário. Quebras de linhas extensas são indicadas por uma barra invertida (\).

```
$ comando -x -y
linha de saída 1
linha de saída 2
linha de saída 3 é muito longa, por isso \
    quebramos para a
linha de saída 3
[...]
linha de saída 98
linha de saída 99
```

Procuramos oferecer descrições curtas para podermos mencionar o maior número possível de utilitários. Para obter mais informações sobre os comandos, consulte as páginas de manual. A maior parte dos comandos também compreende o parâmetro `--help`, que gera uma breve lista de parâmetros possíveis.

25.1 Lista de arquivos abertos: lsof

Para ver uma lista de todos os arquivos abertos para o processo com ID *PID*, use `-p`. Por exemplo, para ver todos os arquivos usados pelo shell atual, digite:

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t
(totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /binzsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so zsh
   4694   jj  mem    REG    3,2   11648    20610
/usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410
/usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393
/usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565
/usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598
/usr/libzsh/4.2.0zsh/computil.so
zsh     4694   jj    0u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48               50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48               50 /dev/pts/48
```

Foi usada a variável de shell especial `$$`, cujo valor é o ID do processo do shell.

O comando `lsof` lista todos os arquivos atualmente abertos quando usado com quaisquer outros parâmetros. Como há milhares de arquivos abertos, raramente é útil listá-los. No entanto, a lista de todos os arquivos pode ser combinada com funções de pesquisa para gerar listas úteis. Por exemplo, listar todos os dispositivos de caracteres usados:

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
```

```
zsh        4694      jj    2u   CHR 136,48                50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48                50 /dev/pts/48
X          6476    root  mem    CHR    1,1             38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48                50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48                50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48                50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48                50 /dev/pts/48
```

25.2 Arquivos de acesso do usuário: fuser

Pode ser útil determinar os processos ou usuários que estão acessando atualmente determinados arquivos. Suponha, por exemplo, que você queira desmontar um sistema de arquivos montado em `/mnt`. `unmount` retorna "device is busy" (dispositivo ocupado). O comando `fuser` pode ser usado para determinar os processos que estão acessando o dispositivo:

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt jj        26597 f....  less
```

Ao fim do processo `less`, que estava sendo executado em outro terminal, o sistema de arquivos poderá ser desmontado com êxito.

25.3 Propriedades de arquivo: stat

O comando `stat` exibe propriedades de arquivo:

```
$ stat xml-doc.txt
File: `xml-doc.txt'
Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

O parâmetro `--filesystem` produz detalhes das propriedades do sistema de arquivos no qual o arquivo específico está localizado:

```
$ stat  . --filesystem
File: "."
```

```
ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Se você usar o shell z (`zsh`), deverá digitar `/usr/bin/stat`, porque o shell z possui um shell interno `stat` com opções e formato de saída diferentes:

```
% type
stat stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

25.4 Dispositivos USB: lsusb

O comando `lsusb` lista todos os dispositivos USB. Com a opção `-v`, imprima uma lista mais detalhada. As informações detalhadas são lidas do diretório `/proc/bus/usb/`. Abaixo é apresentada a saída de `lsusb` após a conexão de um dispositivo de memória USB. As últimas linhas indicam a presença do novo dispositivo.

```
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 001: ID 0000:0000
Bus 001 Device 018: ID 0402:5634 ALi Corp.
```

25.5 Informações sobre um dispositivo SCSI: scsiinfo

O comando `scsiinfo` lista informações sobre um dispositivo SCSI. Com a opção `-l`, liste todos os dispositivos SCSI conhecidos pelo sistema (informações semelhantes são obtidas com o comando `lsscsi`). Veja abaixo a saída de `scsiinfo -i /dev/sda`, que fornece informações sobre o disco rígido. A opção `-a` fornece ainda mais informações.

```
Inquiry command
---------------
Relative Address                    0
Wide bus 32                         0
Wide bus 16                         1
Synchronous neg.                    1
Linked
Commands                     1 Command Queueing                     1
SftRe                               0
Device Type                         0
Peripheral Qualifier                0
Removable?                          0
Device Type Modifier                0
ISO Version                         0
ECMA Version                        0
ANSI Version                        3
AENC                                0
TrmIOP                              0
Response Data Format                2
Vendor:                    FUJITSU
Product:                   MAS3367NP
Revision level:            0104A0K7P43002BE
```

Existe uma lista de defeitos com duas tabelas de blocos defeituosos de um disco rígido: primeiro, o oferecido pelo fornecedor (tabela do fabricante) e, depois, a lista de blocos deficientes que apareceu na operação (tabela de crescimento). Se o número de entradas da tabela de crescimento aumentar, convém substituir o disco rígido.

25.6 Processos: top

O comando `top`, que é o acrônimo de "tabela de processos" em inglês, exibe uma lista de processos que são atualizados a cada dois segundos. Para finalizar o programa,

pressione Q. O parâmetro `-n 1` finaliza o programa após uma única exibição da lista de processos. Veja abaixo um exemplo da saída do comando `top -n 1`:

```
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
  1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0   820  820  612 R  1.0  0.2   0:00.03 top
1 root      15   0   100   96   72 S  0.0  0.0   0:08.43 init
2 root      15   0     0    0    0 S  0.0  0.0   0:04.96 keventd
3 root      34  19     0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
4 root      15   0     0    0    0 S  0.0  0.0   0:33.63 kswapd
5 root      15   0     0    0    0 S  0.0  0.0   0:00.71 bdflush
[...]
1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Se você pressionar F enquanto o comando `top` estiver em execução, aparecerá um menu no qual será possível mudar o formato da saída.

O parâmetro `-U UID` monitora apenas os processos associados a um usuário específico. Substitua *`UID`* pelo ID do usuário. O comando `top -U $(id -u nomedeusu rio)` retorna o UID do usuário em questão e exibe seus processos.

25.7 Lista de processos: ps

O comando `ps` gera uma lista de processos. Se o parâmetro `r` for adicionado, apenas os processos que estiverem usando tempo de computação serão mostrados:

```
$ ps r
PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

Esse parâmetro deve ser escrito sem o sinal de subtração. Os vários parâmetros são escritos algumas vezes com e outras vezes sem o sinal de subtração. A página de manual

pode facilmente afastar usuários potenciais, mas felizmente o comando `ps --help` produz uma página breve de ajuda.

Para verificar quantos processos `emacs` estão em execução, use:

```
$ ps x | grep emacs
1288 ?        S      0:07 emacs
3396 pts/3    S      0:04 emacs new-makedoc.txt
3475 ?        S      0:03 emacs .Xresources
20027 pts/7   S     0:40 emacs xml/common/utilities.xml
20974 pts/7   S     0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

O parâmetro `-p` seleciona processos por meio do ID do processo:

```
$ ps www -p $(pidof xterm)
PID TTY      STAT   TIME COMMAND
9025 ?        S      0:01 xterm -g 100x45+0+200
9176 ?        S      0:00 xterm -g 100x45+0+200
29854 ?        S      0:21 xterm -g 100x75+20+0 -fn \
-B&H-LucidaTypewriter-Medium-R-Normal-Sans-12-120-75-75-M-70-iso10646-1
4378 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -n root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -bg DarkSeaGreen1 -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200 -fn \
lucidasanstypewriter-12
23104 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

A lista de processos pode ser formatada de acordo com suas necessidades. A opção `-L` retorna uma lista com todas as palavras-chave. Digite o comando a seguir para gerar uma lista de todos os processos classificados conforme o uso de memória:

```
$ ps ax --format pid,rss,cmd --sort rss
PID  RSS CMD
2    0 [ksoftirqd/0]
3    0 [events/0]
17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth /var/lib/xdm/authdir/au
```

25.8 Árvore de processos: pstree

O comando `pstree` gera uma lista de processos na forma de árvore:

```
$ pstree
init-+-atd
|-3*[automount]
|-bdflush
|-cron
[...]
|-usb-storage-1
|-usb-storage-2
|-10*[xterm---zsh]
|-xterm---zsh---mutt
|-2*[xterm---su---zsh]
|-xterm---zsh---ssh
|-xterm---zsh---pstree
|-ypbind---ypbind---2*[ypbind]
`-zsh---startx---xinit4-+-X
`-ctwm-+-xclock
|-xload
`-xosview.bin
```

O parâmetro `-p` adiciona o ID do processo a um nome determinado. Para que as linhas de comando também sejam exibidas, use o parâmetro `-a`:

```
$ pstree -pa
init,1
|-atd,1255
[...]
`-zsh,1404
`-startx,1407 /usr/X11R6/bin/startx
`-xinit4,1419 /suse/jj/.xinitrc [...]
|-X,1426 :0 -auth /suse/jj/.Xauthority
`-ctwm,1440
|-xclock,1449 -d -geometry -0+0 -bg grey
|-xload,1450 -scale 2
`-xosview.bin,1451 +net -bat +net
```

25.9 Quem está fazendo o quê: w

Com o comando `w`, você pode saber quem efetuou login no sistema e o que cada usuário está fazendo. Por exemplo:

```
$ w
15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
```

```
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

A última linha mostra que o usuário jj estabeleceu uma conexão de shell segura (`ssh`) com o computador `totan`. Se algum usuário do sistema tiver efetuado login remotamente, o parâmetro `-f` mostrará os computadores dos quais ele estabeleceu a conexão.

25.10 Uso da memória: free

O utilitário `free` examina o uso da RAM. São mostrados detalhes da memória livre e da memória utilizada (em áreas de troca):

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

Com a opção `-m`, todos os tamanhos são expressos em megabytes:

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

A informação realmente interessante vem na próxima linha:

```
-/+ buffers/cache:        191        311
```

Essa linha calcula a quantidade de memória ocupada pelos buffers e caches. O parâmetro `-d delay` assegura que a exibição seja atualizada a cada *atraso* segundos. Por exemplo, `free -d 1.5` produz uma atualização a cada 1,5 segundo.

25.11 Buffer do anel de kernel: dmesg

O kernel Linux mantém certas mensagens em um buffer em anel. Para ver essas mensagens, digite o comando `dmesg`:

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
sdc: I/O error: dev 08:20, sector 0
I/O error: dev 08:20, sector 0
I/O error: dev 08:20, sector 2097144
I/O error: dev 08:20, sector 2097144
I/O error: dev 08:20, sector 0
I/O error: dev 08:20, sector 0
unable to read partition table
I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

A última linha indica que existe um problema temporário no servidor NFS `totan`. As linhas até esse ponto são acionadas pela inserção de uma unidade de memória flash USB. Eventos mais antigos são registrados nos arquivos `/var/log/messages` e `/var/log/warn`.

25.12 Sistemas de arquivos e sua utilização: mount, df e du

O comando `mount` mostra o sistema de arquivos (dispositivo e tipo) que está montado e seu ponto de montagem:

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
```

```
 (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
(rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

Obtenha informações sobre a utilização total dos sistemas de arquivos com o comando `df`. O parâmetro `-h` (ou `--human-readable`) transforma a saída em um formato inteligível para o usuário comum.

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Os usuários do servidor de arquivos NFS `totan` devem limpar seus diretórios principais imediatamente. Exiba o tamanho total de todos os arquivos de um determinado diretório e seus subdiretórios com o comando `du`. O parâmetro `-s` suprime a saída de informações detalhadas. `-h` novamente transforma os dados em um formato compreensível para o usuário comum. Com este comando:

```
$ du -sh ~
361M    /suse/jj
```

veja o espaço ocupado por seu próprio diretório principal.

25.13 O sistema de arquivos /proc

O sistema de arquivos `/proc` é um pseudossistema de arquivos no qual o kernel reserva informações importantes na forma de arquivos virtuais. Por exemplo, exiba o tipo de CPU com este comando:

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

A alocação e o uso de interrupções podem ser consultados com o seguinte comando:

```
$ cat /proc/interrupts
CPU0
0:  537544462          XT-PIC  timer
1:     820082          XT-PIC  keyboard
2:          0          XT-PIC  cascade
8:          2          XT-PIC  rtc
9:          0          XT-PIC  acpi
10:      13970           XT-PIC  usb-uhci, usb-uhci
11:  146467509           XT-PIC  ehci_hcd, usb-uhci, eth0
12:    8061393           XT-PIC  PS/2 Mouse
14:    2465743           XT-PIC  ide0
15:       1355           XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Alguns arquivos importantes e seu conteúdo:

/proc/devices
: dispositivos disponíveis

/proc/modules
: módulos kernel carregados

/proc/cmdline
: linha de comando do kernel

/proc/meminfo
: detalhes sobre a utilização da memória

/proc/config.gz
: arquivo de configuração `gzip` compactado do kernel executado atualmente

Mais informações estão disponíveis no arquivo de texto `/usr/src/linux/Documentation/filesystems/proc.txt`. Você pode encontrar informações sobre os processos em execução nos diretórios `/proc/`*`NNN`*, onde *`NNN`* é o ID do processo (PID) relevante. Cada processo pode encontrar suas próprias características em `/proc/self/`:

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
```

```
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

A atribuição de endereço de executáveis e bibliotecas pode ser encontrada no arquivo `maps`:

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

25.14 vmstat, iostat e mpstat

O utilitário `vmstat` reporta estatísticas da memória virtual. Ele lê os arquivos `/proc/meminfo`, `/proc/stat` e `/proc/*/stat`. É útil para identificar gargalos no desempenho do sistema. O comando `iostat` reporta estatísticas sobre a CPU e a entrada e saída de dispositivos e partições. As informações exibidas são obtidas dos arquivos `/proc/stat` e `/proc/partitions`. A saída pode ser usada para equilibrar melhor a entrada e a saída de carga entre os discos rígidos. O comando `mpstat` reporta estatísticas referentes à CPU.

25.15 procinfo

Informações importantes do sistema de arquivos `/proc` são resumidas pelo comando `procinfo`:

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]


Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :        0
nice  :       0:31:57.13   0.2%  page out:        0
system:       0:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498

irq  0: 776561217 timer                  irq  8:          2 rtc

irq  1:    276048 i8042                  irq  9:      24300 VIA8233

irq  2:         0 cascade [4]           irq 11:  38610118 acpi, eth0, uhci_hcd

irq  3:         3                        irq 12:   3435071 i8042

irq  4:         3                        irq 14:   2236471 ide0

irq  6:         2                        irq 15:       251 ide1
```

Para ver todas as informações, use o parâmetro `-a`. O parâmetro `-nN` produz atualizações das informações a cada *N* segundos. Nesse caso, termine o programa pressionando Q.

Por padrão, são exibidos valores cumulativos. O parâmetro `-d` produz valores diferenciais. `procinfo -dn5` exibe os valores modificados nos últimos cinco segundos:

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
```

```
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer
irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard
irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]
irq 12:       132 PS/2 Mouse irq  6:         0                      irq 14:         0
 ide0 irq  8:         0 rtc                   irq 15:         0 ide1 irq  9:         0
 acpi
```

25.16 Recursos PCI: lspci

O comando `lspci` lista os recursos PCI:

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \ VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \ VT8366/A/7 [Apollo KT266/A/333
AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \ DECchip 21140
[FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \ PIPC Bus
Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \ VT8233 AC97
Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \ MGA G550 AGP (rev
 01)
```

Usar `-v` resulta em uma lista mais detalhada:

```
$ lspci -v
[...]
01:00.0 \ VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev
 01) \ (prog-if 00 [VGA]) Subsystem: Matrox Graphics, Inc. Millennium G550
Dual Head DDR 32Mb Flags: bus master, medium devsel, latency 32, IRQ 10 Memory
 at d8000000 (32-bit, prefetchable) [size=32M] Memory at da000000 (32-bit,
non-prefetchable) [size=16K] Memory at db000000 (32-bit, non-prefetchable)
[size=8M] Expansion ROM at <unassigned> [disabled] [size=128K] Capabilities:
 <available only to root>
```

Informações sobre a resolução de nomes do dispositivo podem ser obtidas do arquivo `/usr/share/pci.ids`. Os IDs do PCI não listados nesse arquivo são marcados como “Unknown device” (arquivo desconhecido).

O parâmetro `-w` produz todas as informações que poderiam ser consultadas pelo programa. Para ver valores puramente numéricos, use o parâmetro `-n`.

25.17 Chamadas do sistema de uma execução de programa: strace

O utilitário `strace` permite rastrear todas as chamadas do sistema de um processo em execução. Digite o comando normalmente, adicionando `strace` ao início da linha:

```
$ strace -e open ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
 = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
= 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Por exemplo, para rastrear todas as tentativas de abertura de um arquivo específico, use:

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
```

```
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Para rastrear todos os processos-filho, use o parâmetro `-f`. O comportamento e o formato da saída de strace podem ser amplamente controlados. Para obter informações, consulte `man strace`.

25.18 Chamadas da biblioteca de uma execução de programa: ltrace

O comando `ltrace` permite rastrear as chamadas de biblioteca de um processo. Esse comando é usado de forma semelhante a `strace`. O parâmetro `-c` gera o número e a duração das chamadas de biblioteca ocorridas:

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
86.27    1.071814          30     35327           write
10.15    0.126092          38      3297           getdents64
2.33     0.028931           3     10208           lstat64
0.55     0.006861           2      3122         1 chdir
0.39     0.004890           3      1567         2 open
[...]
0.00     0.000003           3         1           uname
0.00     0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

25.19 Especificação da biblioteca necessária: ldd

O comando `ldd` pode ser usado para descobrir as bibliotecas que carregariam o executável dinâmico especificado como argumento:

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
```

```
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Binários estáticos não precisam de bibliotecas dinâmicas:

```
$ ldd /bin/sash
 not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

25.20 Informações adicionais sobre binários ELF

O conteúdo dos binários pode ser lido com o utilitário `readelf`. Isso também funciona com arquivos ELF criados para outras arquiteturas de hardware:

```
$ readelf --file-header /bin/ls
ELF Header:
Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
Class:                             ELF32
Data:                              2's complement, little endian
Version:                           1 (current)
OS/ABI:                            UNIX - System V
ABI Version:                       0
Type:                              EXEC (Executable file)
Machine:                           Intel 80386
Version:                           0x1
Entry point address:               0x8049b40
Start of program headers:          52 (bytes into file)
Start of section headers:          76192 (bytes into file)
Flags:                             0x0
Size of this header:               52 (bytes)
Size of program headers:           32 (bytes)
Number of program headers:         9
Size of section headers:           40 (bytes)
Number of section headers:         29
Section header string table index: 26
```

25.21 Comunicação entre processos: ipcs

O comando `ipcs` produz uma lista dos recursos IPC em uso:

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

25.22 Medição do tempo com time

O tempo usado pelos comandos pode ser determinado com o utilitário `time`. Esse utilitário está disponível em duas versões: como shell interno e como programa (`/usr/bin/time`).

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Parte VIII Sistema

26 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits

O SUSE Linux está disponível para várias plataformas de 64 bits. Isso não significa necessariamente que todos os aplicativos incluídos tenham sido transpostos para plataformas de 64 bits. O SUSE Linux suporta o uso de aplicativos de 32 bits em um ambiente de sistema de 64 bits. Este capítulo oferece uma breve visão geral de como este suporte é implementado em plataformas Linux de 64 bits. Ele explica como aplicativos de 32 bits são executados (suporte do tempo de execução) e como aplicativos de 32 bits devem ser compilados para que possam ser executados em ambientes de sistema de 32 bits e 64 bits. Além disso, você vai encontrar informações sobre API do Kernel e uma explicação sobre como aplicativos de 32 bits podem ser executados com um kernel de 64 bits.

O SUSE Linux para as plataformas de 64 bits AMD64 e EM64T foi criado para que os aplicativos de 32 bits existentes sejam executados no ambiente de 64 bits "sem necessidade de mudanças". Este suporte significa que você pode continuar a usar os aplicativos de 32 bits de sua preferência sem esperar que uma porta de 64 bits correspondente se torne disponível.

26.1 Suporte ao tempo de execução

IMPORTANTE: Conflitos entre versões de aplicativos

Se um aplicativo estiver disponível para ambientes de 32 bits e de 64 bits, a instalação paralela das duas versões provavelmente resultará em problemas. Em tais casos, opte pela instalação e pelo uso de uma das duas versões.

Para que os aplicativos sejam executados corretamente, cada um deles requer uma variedade de bibliotecas. Infelizmente, os nomes das versões de 32 bits e 64 bits das bibliotecas são idênticos. Eles devem ser diferenciados uns dos outros de outra forma.

Para obter compatibilidade com a versão de 32 bits, as bibliotecas são armazenadas no mesmo local no sistema e no ambiente de 32 bits. A versão de 32 bits de `libc.so.6` está localizada em `/lib/libc.so.6` nos ambientes de 32 bits e 64 bits.

Todos os arquivos de objetos e todas as bibliotecas de 64 bits estão localizados em diretórios denominados `lib64`. Os arquivos de objetos de 64 bits que normalmente são encontrados em `/lib`, `/usr/lib` e `usr/X11R6/lib` agora estão em `/lib64`, `/usr/lib64` e `/usr/X11R6/lib64`. Isso significa que há espaço para bibliotecas de 32 bits em `/lib` `/usr/lib` e `/usr/X11R6/lib`, de forma que os nomes de arquivo das duas versões possam permanecer inalterados.

Nenhum subdiretório dos diretórios de objetos cujo conteúdo de dados não dependa do tamanho da palavra será movido. Por exemplo, as fontes X11 ainda se encontram no local habitual, em `/usr/X11R6/lib/X11/fonts`. Este esquema está em conformidade com a LSB (Linux Standards Base - Base de padrões Linux) e com o FHS (File System Hierarchy Standard - Padrão de hierarquia de sistema de arquivos).

26.2 Desenvolvimento de software

Uma cadeia de ferramentas de desenvolvimento biarch permite a geração de objetos de 32 bits e 64 bits. O padrão é compilar objetos de 64 bits. É possível gerar objetos de 32 bits usando sinalizadores especiais. Para GCC, o sinalizador especial é `-m32`.

Todos os arquivos de cabeçalho devem ser escritos em um formato independente de arquitetura. As bibliotecas de 32 bits e 64 bits instaladas devem ter uma API (application programming interface - interface de programação de aplicativo) que corresponda aos arquivos de cabeçalho instalados. O ambiente SUSE normal é projetado de acordo com esse princípio. No caso de bibliotecas atualizadas manualmente, solucione esses problemas por conta própria.

26.3 Compilação de software em plataformas biarch

Para desenvolver binários para outra arquitetura em uma arquitetura biarch, as respectivas bibliotecas da segunda arquitetura devem ser instaladas adicionalmente. Esses pacotes são chamados de `rpmname-32bit`. Você também precisará dos respectivos cabeçalhos e bibliotecas dos pacotes `rpmname-devel` e das bibliotecas de desenvolvimento para a segunda arquitetura de `rpmname-devel-32bit`.

A maioria dos programas de código-fonte aberto usa uma configuração de programa baseada em `autoconf`. Para usar o `autoconf` com o objetivo de configurar um programa para a segunda arquitetura, sobregrave as configurações do compilador normal e do linker de `autocong` executando o script `configure` com variáveis de ambiente adicionais.

Os exemplos a seguir se referem a um sistema AMD64 ou EM64T com x86 como segunda arquitetura:

1. Defina `autoconf` para usar o compilador de 32 bits:

   ```
   CC="gcc -m32"
   ```

2. Instrua o linker a processar objetos de 32 bits:

   ```
   LD="ld -m elf64_i386"
   ```

3. Defina o assembler para gerar objetos de 32 bits:

   ```
   AS="gcc -c -m32"
   ```

4. Determine que as bibliotecas para `libtool` e as demais venham de `/usr/lib`:

   ```
   LDFLAGS="-L/usr/lib"
   ```

5. Determine que as bibliotecas sejam armazenadas no subdiretório `lib`:

   ```
   --libdir=/usr/lib
   ```

6. Determine que as bibliotecas X de 32 bits sejam usadas:

```
      --x-libraries=/usr/X11R6/lib/
```

Nem todas essas variáveis são necessárias para todos os programas. Adapte-as para o respectivo programa.

```
CC="gcc -m64"            \
LDFLAGS="-L/usr/lib64;"  \
        .configure       \
          --prefix=/usr  \
          --libdir=/usr/lib64
make
make install
```

26.4 Especificações do kernel

Os kernels de 64 bits para AMD64 e EM64T oferecem uma ABI (application binary interface - interface binária de aplicativo) de kernel de 32 bits e de 64 bits. A de 64 bits é idêntica à ABI do kernel de 32 bits correspondente. Isso significa que o aplicativo de 32 bits pode se comunicar com o kernel de 64 bits da mesma forma que com o kernel de 32 bits.

A emulação de 32 bits de chamadas do sistema para um kernel de 64 bits não suporta várias APIs usadas pelos programas do sistema. Isso depende da plataforma. Por esta razão, alguns aplicativos, como `lspci` ou os programas de administração LVM, devem ser compilados como programas de 64 bits para funcionar adequadamente.

Um kernel de 64 bits só pode carregar módulos de kernel de 64 bits especificamente compilados para esse kernel. Não é possível usar módulos de kernel de 32 bits.

DICA

Alguns aplicativos requerem módulos separados carregáveis pelo kernel. Se você pretende usar um aplicativo de 32 bits desse tipo em um ambiente de sistema de 64 bits, entre em contato com o provedor do aplicativo e do SUSE para verificar se a versão de 64 bits do módulo carregável pelo kernel e a versão compilada de 32 bits da API do kernel estão disponíveis para esse módulo.

27 Trabalhando com o Shell

As interfaces gráficas de usuário estão ficando cada vez mais importantes para o Linux, mas usar o mouse nem sempre é a melhor forma de realizar as tarefas diárias. A linha de comando oferece alta flexibilidade e eficiência. Os aplicativos baseados em texto são principalmente importantes para controlar computadores em links de rede lentos ou se você deseja executar tarefas como `root` na linha de comando em um xterm. O shell Bash é o interpretador de linha de comando padrão no SUSE Linux.

Linux é um sistema multiusuário e o acesso a arquivos é controlado pelas permissões do usuário. Independentemente de usar a linha de comando ou uma interface gráfica de usuário, é útil entender o conceito de permissão. Ao usar a linha de comando, um número de comandos são importantes. O editor de textos vi geralmente é usado ao configurar um sistema a partir da linha de comando. Ele também é conhecido por vários administradores do sistema e desenvolvedores.

27.1 Usando Bash na linha de comando

Na barra de tarefas do KDE, existe um ícone que ilustra um monitor com uma concha. Quando você clica nesse ícone, uma janela de terminal é aberta para a digitação de comandos. O Konsole, o programa de terminal, normalmente executa o Bash (Bourne again shell), um programa desenvolvido como parte do projeto GNU. Na área de trabalho GNOME, clique no ícone de monitor de computador no painel superior para iniciar um terminal que normalmente executa o Bash.

Depois de abrir o shell, veja a primeira linha do prompt. O prompt geralmente consiste no nome do usuário, nome do host e no caminho atual, mas pode ser personalizado. Quando o cursor está depois desse prompt, você pode enviar comandos diretamente ao seu sistema de computador.

27.1.1 Digitando comandos

Um comando é composto de vários elementos. O primeiro elemento é sempre o comando real, seguido por parâmetros e opções. Os comandos são executados quando você pressiona Enter. Antes disso, você pode editar a linha de comando, adicionar opções ou corrigir erros de digitação com facilidade. Um dos comandos mais usados é o `ls`, que pode ser usado com ou sem argumentos. Digitar o comando `ls` simples no console mostra o conteúdo do diretório atual.

As opções são prefixadas com hífen. O comando `ls -l`, por exemplo, mostra o conteúdo do mesmo diretório em detalhes (formato de listagem longa). Ao lado de cada nome de arquivo, você pode ver sua data de criação, seu tamanho em bytes e mais detalhes, que serão abordados mais adiante. Uma opção muito importante que existe para vários comandos é `--help`. Quando você digita `ls --help`, todas as opções do comando `ls` são exibidas.

É importante usar as "aspas" corretamente. Se um nome de arquivo contiver um espaço, anule o espaço usando uma barra invertida (`\`) ou delimite o nome do arquivo entre aspas simples ou duplas. Caso contrário, o Bash interpretará um nome de arquivo como `Meus Documentos` como os nomes de dois arquivos ou diretórios. A diferença entre as aspas simples e duplas é que a expansão de variáveis ocorre dentro de aspas duplas. As aspas simples garantem que o shell veja a string com aspas de forma literal.

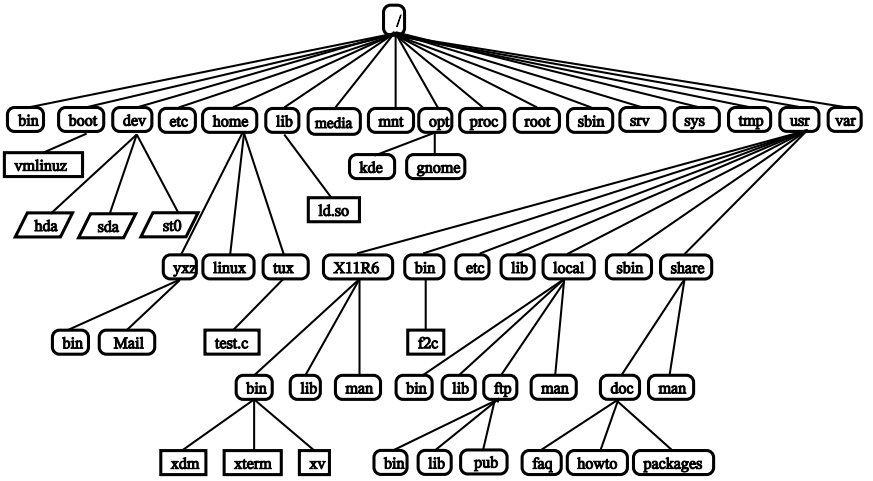
27.1.2 Arquivos e diretórios

Para usar o shell de forma eficaz, é muito útil conhecer um pouco sobre as estruturas de arquivos e diretórios do sistema Linux. Você pode considerar os diretórios como pastas eletrônicas nas quais são armazenados arquivos, programas e subdiretórios. O diretório de nível superior na hierarquia é o diretório raiz, indicado como `/`. É a partir dele que todos os outros diretórios podem ser acessados.

O diretório `/home` contém os diretórios em que os usuários individuais podem armazenar seus arquivos pessoais. Figura 27.1, "Exemplo de uma árvore de diretórios

padrão" (p 405) mostra a árvore de diretórios padrão no Linux, com os diretórios pessoais dos usuários de exemplo `xyz`, `linux` e `tux`. A árvore de diretórios do sistema Linux tem uma estrutura funcional que segue o *FHS (Filesystem Hierarchy Standard - Padrão da Hierarquia do Sistema de Arquivos)*. A lista abaixo oferece uma breve descrição dos diretórios padrão do Linux.

Figura 27.1 *Exemplo de uma árvore de diretórios padrão*



/
Diretório raiz, ponto inicial da árvore de diretórios

/home
Diretórios pessoais de usuários

/dev
Arquivos de dispositivos que representam componentes de hardware

/etc
Arquivos importantes para a configuração do sistema

/etc/init.d
Scripts de boot

/usr/bin
Programas genericamente acessíveis

/bin
Programas necessários anteriormente no processo de boot

/usr/bin
Programas reservados ao administrador do sistema

/sbin
Programas reservados ao administrador do sistema e necessários para inicialização

/usr/include
Arquivos de cabeçalho para o compilador C

/usr/include/g++
Arquivos de cabeçalho para o compilador C++

/usr/share/doc
Arquivos de documentação variados

/usr/share/man
Páginas do manual do sistema (páginas de manual)

/usr/src
Código-fonte do software do sistema

/usr/src/linux
Código-fonte do kernel

/tmp, /var/tmp
Arquivos temporários

/usr
Todos os programas aplicativos

/var
Arquivos de configuração (por exemplo, aqueles vinculados de `/usr`)

/var/log
Arquivos de registro do sistema

/var/adm
Dados do administrador do sistema

/lib
Bibliotecas compartilhadas (para programas vinculados dinamicamente)

/proc
Sistema de arquivos de processamento

/sys
Sistema de arquivos do sistema em que são reunidas todas as informações sobre dispositivos do kernel

/usr/local
Local, extensões independentes de distribuição

/opt
Software opcional, pacotes de programas complementares maiores (como KDE, GNOME, Netscape)

27.1.3 Recursos do Bash

Há dois recursos importantes do shell que podem facilitar o seu trabalho:

Histórico
Para repetir um comando que tenha sido digitado anteriormente, pressione ↑ até o comando anterior aparecer no prompt. Mova para o próximo da lista de comandos digitados anteriormente pressionando ↓. Para editar a linha de comando, mova o cursor até a posição desejada usando as teclas de seta e inicie a digitação. Use Ctrl + R para pesquisar o histórico.

Finalização
Finalize o nome do arquivo após digitar suas primeiras letras até que ele possa ser identificado com exclusividade. Para isso, digite as primeiras letras e pressione Tab. Se houver vários nomes de arquivo iniciando com as mesmas letras, obtenha uma lista de tais nomes pressionando Tab duas vezes.

Primeiro exemplo: Gerenciando arquivos

Agora que você já sabe qual é a aparência de um comando, conhece os diretórios do SUSE Linux e sabe como agilizar procedimentos usando o Bash, coloque esse conhecimento em prática neste pequeno exercício.

1. Abra um console na área de trabalho do KDE OU GNOME clicando no ícone de concha.

2. Digite o comando `ls` para ver o conteúdo do seu diretório pessoal.

3. Use o comando `mkdir` (que significa *criar diretório*) para criar um novo subdiretório chamado `test` digitando `mkdir test`.

4. Agora, inicie um editor pressionando Alt + F2 e digitando `kate` Kate para KDE `gedit` para Gedit no GNOME. Digite algumas letras no editor e salve o arquivo como `Testfile` no seu diretório pessoal. O Linux diferencia maiúsculas de minúsculas. Por exemplo, use um T maiúsculo.

5. Exiba o conteúdo do seu diretório pessoal novamente. Em vez de digitar `ls` mais uma vez, pressione ↑ duas vezes e o comando `ls` reaparecerá no prompt. Para executar o comando, pressione Enter. O diretório `test` recém-criado deverá aparecer em letras azuis e `Testfile` em letras pretas. É dessa forma que diferenciamos diretórios de arquivos em um console.

6. Mova `Testfile` para o subdiretório `test` com o comando `mv`. Para agilizar o processo, use a função de expansão: digite `mv T` e pressione Tab. Se não houver outro arquivo cujo nome comece com essa letra no diretório, o shell expandirá o nome do arquivo e adicionará a string *estfile*. Caso contrário, adicione uma ou duas letras por conta própria e experimente pressionar Tab todas as vezes para ver se o shell expande o nome. Por fim, digite um espaço e `test` após o nome do arquivo expandido e pressione Enter para executar o comando.

7. Nesse momento, o `Testfile` provavelmente não estará mais no diretório. Digite `ls` novamente para verificar se realmente não está.

8. Para ver se o arquivo foi de fato movido, vá para o diretório `test` com o comando `cd test`. Digite `ls` novamente. Você deverá ver `Testfile` na listagem. Volte para o seu diretório pessoal em qualquer ponto digitando apenas `cd`.

9. Para fazer cópia de um arquivo, use `cp`. Por exemplo, digite `cp Testfile Testbackup` para copiar o `Testfile` para o `Testbackup`. Mais uma vez, o comando `ls` pode ser usado para constatar se os arquivos estão nos diretórios.

27.1.4 Especificando caminhos

Quando você estiver trabalhando com arquivos ou diretórios, é importante especificar o caminho correto. Entretanto, você não precisa digitar o caminho completo (absoluto) desde o diretório raiz até o respectivo arquivo. Você pode iniciar no diretório atual. Acesse seu diretório pessoal diretamente com `~`. Isso significa que há duas maneiras de listar o arquivo `Testfile` no diretório `test`: digitando o caminho relativo com o comando `ls test` ou especificando o caminho absoluto com `ls ~/test`.

Para relacionar o conteúdo dos diretórios pessoais dos outros usuários, digite `ls ~nomedousu rio`. Na árvore de diretórios mencionada acima, um dos usuários de exemplo é `tux`. Nesse caso, `ls ~tux` relacionaria o conteúdo do diretório pessoal de `tux`.

Faça referência ao diretório atual com um ponto (`.`). O próximo nível superior na árvore é representado por dois pontos (`..`). Digitando `ls ..`, veja o conteúdo do diretório pai do diretório atual. O comando `ls ../..` mostra o conteúdo do diretório dois níveis acima na hierarquia.

Segundo exemplo: Trabalhando com caminhos

Veja aqui outro exemplo que ilustra como percorrer os diretórios do sistema SUSE Linux.

1. Vá para o seu diretório pessoal com o comando `cd`. Em seguida, crie um diretório com o nome `test2` digitando `mkdir test2`.

2. Vá para o novo diretório com o comando `cd test2` e crie nele um subdiretório com o nome `subdirectory`. Para ir até ele, use a função de expansão: digite `cd su` e pressione Tab. O shell expandirá o restante do nome do diretório.

3. Agora tente mover o arquivo criado anteriormente `Testbackup` para o diretório atual (`subdirectory`) sem mudar o diretório novamente. Para isso, especifique o caminho relativo desse arquivo: `mv ../../test/Testbackup .` (observe o ponto no final). O ponto no fim do comando é necessário para informar ao shell que o diretório atual é o destino do arquivo. `../../`, neste exemplo, refere-se ao seu diretório pessoal.

27.1.5 Curingas

Outra vantagem oferecida pelo shell são os curingas para a expansão de nomes de caminho. Existem três tipos diferentes no Bash:

?
: Corresponde exatamente a um caractere arbitrário.

*****
: Corresponde a qualquer número de caracteres

[set]
: Corresponde a um dos caracteres do grupo especificado entre os colchetes, que aqui é representado pela string *set*. Com parte de *set* , você também pode especificar as classes de caractere usando a sintaxe *[:classe:]*, onde a classe pode ser `alnum`, `alpha`, `ascii` etc.

  Se você usar `!` ou `^` no início do grupo (*[!set]*), haverá correspondência com um caractere diferente daqueles identificados por *set*.

Pressupondo-se que o diretório `test` contenha os arquivos `Testfile`, `Testfile1`, `Testfile2` e `datafile`, o comando `ls Testfile?` listará os arquivos `Testfile1` e `Testfile2`. Com `ls Test*`, a lista também incluirá `Testfile`. `ls *fil*` mostra todos os arquivos de exemplo. Por fim, você pode usar o curinga `set` para acessar todos os arquivos de exemplo cujo último caractere é um número: `ls Testfile[1-9]` ou, usando classes, `ls Testfile[[:digit:]]`.

Dos quatro tipos de curingas, o mais inclusivo é o asterisco. Ele pode ser usado para copiar todos os arquivos contidos em um diretório para outro diretório ou apagar todos os arquivos com um único comando. O comando `rm *fil*`, por exemplo, apaga todos os arquivos do diretório cujo nome inclua a string *fil*.

27.1.6 Less (Menos) e More (Mais)

O Linux inclui dois programas pequenos para a exibição de arquivos de texto diretamente no shell. Em vez de iniciar um editor para ler um arquivo como `Readme.txt`, basta digitar `less Readme.txt` para exibir o texto na janela de console. Use Space para rolar uma página para baixo. Use as teclas Page Up e Page Down para mover o texto para frente ou para trás. Para sair do programa less, pressione Q.

Em vez de less, você também pode usar o programa mais antigo more. Entretanto, é menos conveniente porque ele não permite que você role para trás.

O programa less recebeu esse nome devido ao preceito de que *menos é mais*. Ele também pode ser usado para ver a saída de comandos de forma conveniente. Para verificar como isso funciona, leia Seção 27.1.7, “Pipes e redirecionamento” (p 411).

27.1.7 Pipes e redirecionamento

Normalmente, a saída padrão no shell é a sua tela ou a janela de console, e a entrada padrão é o teclado. Para encaminhar a saída de um comando para um aplicativo como less, use um *pipeline*.

Para ver os arquivos no diretório `test`, digite o comando `ls test | less`. O conteúdo do diretório `test` será exibido por meio do less. Isso é recomendável quando a saída normal com `ls` é muito extensa. Por exemplo, se você vir o conteúdo do diretório `dev` com `ls /dev`, apenas uma pequena parte da janela estará visível. Exiba a lista toda com `ls /dev | less`.

Também é possível salvar a saída de comandos em um arquivo. Por exemplo, `echo "test one" > Content` genera um novo arquivo chamado `Content` que contém as palavras `test one`. Exiba o arquivo com `less Content`.

Você também pode usar um arquivo como a entrada de um comando. Por exemplo, com `tr`, substitua os caracteres da entrada padrão redirecionada do arquivo `Content` e grave o resultado na saída padrão: substitua `t` por `x` chamando `tr t x < Content`. A saída do comando `tr` é enviada para a tela.

Se você precisar de um novo arquivo que contenha a saída, direcione a saída do comando `tr` para um arquivo. Para testar isso, vá para `test` e digite o comando `tr t x < ../Content > new`. Por fim, exiba `new` com `less new`.

Assim como na saída padrão, a saída de erro padrão é enviada para o console. Entretanto, para redirecionar a saída de erro padrão para um arquivo chamado `errors`, acrescente `2> errors` ao comando correspondente. A saída padrão e o erro padrão serão salvos em um arquivo chamado `alloutput` se você acrescentar `>& alloutput`. Por fim, para acrescentar a saída de um comando a um arquivo já existente, o comando deve ser seguido por >> em vez de um único >.

27.1.8 Pacotes e compactação de dados

Agora que você já criou vários arquivos e diretórios, pense em criar pacotes e compactar dados. Suponhamos que você queira que o diretório `test` inteiro seja compactado em um arquivo que possa ser salvo em um chaveiro USB como uma cópia de backup ou enviado por e-mail. Para isso, use o comando `tar` (para o *copiador em fita*). Com `tar --help`, exiba todas as opções do comando `tar`. As opções mais importantes serão explicadas aqui:

-c
(para criação) Cria um novo arquivo.

-t
(para tabela) Exibe o conteúdo de um pacote.

-x
(para extração) Descompacta o pacote.

-v
(para detalhes) Mostra na tela todos os arquivos durante a criação do pacote.

-f
(para arquivo) Escolhe um nome para o arquivo do pacote. Quando você estiver criando um pacote, esta opção deverá ser sempre a última a ser especificada.

Para compactar o diretório `test` com todos os arquivos e subdiretórios em um arquivo denominado `testarchive.tar`, use as opções `-c` e `-f`. Para fins de teste, adicione também `-v` para continuar com o empacotamento, embora esta opção não seja obrigatória. Depois de usar `cd` para mudar para o seu diretório pessoal, onde o diretório `test` está localizado, digite `tar -cvf testarchive.tar test`. Em seguida, exiba o conteúdo do arquivo do pacote com `tar -tf testarchive.tar`. O diretório `test` com todos esses arquivos e diretórios permaneceu inalterado no disco rígido. Para descompactar o arquivo, digite `tar -xvf testarchive.tar`, mas não faça isso ainda.

No caso de compactação de arquivos, a escolha óbvia é `gzip` ou, para uma taxa de compactação ainda melhor, `bzip2`. Digite apenas `gzip testarchive.tar` (ou `bzip2 testarchive.tar`, mas `gzip` é usado neste exemplo). Com o comando `ls`, observe que o arquivo `testarchive.tar` não existe mais e que o arquivo

testarchive.tar.gz foi criado. Esse arquivo é bem menor e, portanto, mais adequado para transferência por e-mail ou armazenamento em um chaveiro USB.

Agora, descompacte o arquivo no diretório test2 criado anteriormente. Para isso, digite cp testarchive.tar.gz test2 para copiar o arquivo para esse diretório. Mude para o diretório usando cd test2. Um arquivo compactado com a extensão .tar.gz pode ser descompactado com o comando gunzip. Digite gunzip testarchive.tar.gz, que resulta no arquivo testarchive.tar, e depois extraia ou *descompacte o tar* usando o comando tar –xvf testarchive.tar. Você também pode descompactar e extrair o arquivo compactado em uma única etapa com tar –xvf testarchive.tar.gz (não é mais necessário adicionar a opção –z). Com ls, observe que um novo diretório test foi criado com o mesmo conteúdo do diretório test no seu diretório pessoal.

27.1.9 mtools

mtools consiste em um conjunto de comandos para se trabalhar com os sistemas de arquivos do MS-DOS. Os comandos incluídos em mtools permitem que você se refira à primeira unidade de disquete como a:, assim como no MS-DOS. Além disso, os comandos se assemelham aos do MS-DOS, exceto pelo fato de que eles são iniciados com o prefixo m:

mdir a:
Exibe o conteúdo do disquete na unidade a:

mcopy Testfile a:
Copia o arquivo Testfile para o disquete

mdel a:Testfile
Apaga o Testfile em a:

mformat a:
Formata o disquete no formato MS-DOS (usando o comando fdformat)

mcd a:
Faz com que a: seja seu diretório atual

mmd a:test
Cria o subdiretório test no disquete

`mrd a:test`
Apaga o subdiretório `test` do disquete

27.1.10 Limpando

Após este curso rápido, você deverá estar familiarizado com as noções básicas sobre a linha de comando ou o shell do Linux. Convém limpar o seu diretório pessoal apagando vários arquivos de teste e diretórios com os comandos `rm` e `rmdir`. Em Seção 27.3, "Comandos importantes do Linux" (p 420), localize uma lista dos comandos mais importantes e uma breve descrição de suas funções.

27.2 Usuários e permissões de acesso

Desde o seu lançamento no início dos anos 90, o Linux foi desenvolvido como um sistema multiusuário. Um número ilimitado de usuários pode trabalhar no Linux simultaneamente. Os usuários precisam efetuar login no sistema antes de iniciar uma sessão na estação de trabalho. Cada usuário possui um nome de usuário com uma senha correspondente. Essa diferenciação entre usuários garante que aqueles não autorizados não possam ver os arquivos aos quais não têm permissão. Mudanças maiores no sistema, como instalações de novos programas, geralmente também são inviáveis ou restritas para usuários normais. Somente o usuário, ou *superusuário*, possui capacidade irrestrita de efetuar mudanças no sistema e tem acesso ilimitado a todos esses arquivos. Aqueles que usam esse conceito com discernimento, apenas efetuando login com acesso total de `root` quando necessário, podem evitar a perda não intencional de dados. Em circunstâncias normais, somente o root pode apagar arquivos de sistema ou formatar discos rígidos. Portanto, a ameaça do *efeito do Cavalo de Tróia* ou da digitação acidental de comandos destrutivos pode ser consideravelmente reduzida.

27.2.1 Permissões do sistema de arquivos

Basicamente, todo arquivo em um sistema de arquivos do Linux pertence a um usuário e a um grupo. Os grupos proprietários e todos os outros podem ser autorizados a gravar, ler ou executar esses arquivos.

Nesse caso, um grupo pode ser definido como um conjunto de usuários conectados que têm determinados direitos coletivos. Por exemplo, chame um grupo que trabalhe em determinado projeto de `project3`. Cada usuário de um sistema Linux é um membro de pelo menos um grupo proprietário, normalmente `users`. Podem existir quantos grupos forem necessários no sistema, mas somente o `root` é capaz de adicionar grupos. Com o comando `groups`, todo usuário pode descobrir de quais grupos ele faz parte.

Acesso a arquivos

A organização das permissões em sistemas de arquivos pode ser diferente para arquivos e diretórios. As informações sobre permissões de arquivos podem ser exibidas com o comando `ls -l`. A saída pode aparecer como no Exemplo 27.1, "Exemplo de saída com permissões de arquivos" (p 415).

Exemplo 27.1 *Exemplo de saída com permissões de arquivos*

```
-rw-r----- 1 tux project3 14197 Jun 21  15:03 Roadmap
```

Como indica a terceira coluna, esse arquivo pertence ao usuário `tux`. Ele está atribuído ao grupo `project3`. Para descobrir as permissões de usuário do arquivo `Roadmap`, a primeira coluna deve ser examinada com mais cuidado.

-	rw-	r--	---
Tipo	Permissões de usuários	Permissões de grupo	Permissões para outros usuários

Essa coluna contém um caractere inicial seguido de nove caracteres agrupados em três. A primeira das dez letras representa o tipo de componente do sistema de arquivos. O travessão (`-`) mostra que este é um arquivo. Um diretório (`d`), um link (`l`), um dispositivo de bloco (`b`) ou um dispositivo de caractere também poderia ser indicado.

Os três próximos blocos seguem um padrão. Os três primeiros caracteres indicam se o arquivo é legível (`r`) ou não (`-`). Um `w` na posição central significa que o objeto correspondente pode ser editado, e um travessão (`-`) significa que não é possível gravá-lo no arquivo. Um `x` na terceira posição significa que o objeto pode ser executado. Como o arquivo do exemplo é um arquivo de texto, e não um executável, o acesso executável a esse arquivo específico não é necessário.

Neste exemplo, `tux` possui, como proprietário do arquivo `Roadmap`, acesso de leitura (`r`) e gravação (`w`), mas não pode executá-lo (`x`). Os membros do grupo `project3` podem ler o arquivo, mas não podem modificá-lo ou executá-lo. Outros usuários não têm qualquer tipo de acesso a esse arquivo. Outras permissões podem ser atribuídas por meio de ACLs (Access Control Lists). Consulte a Seção 27.2.6, "Listas de controle de acesso" (p 419) para obter mais informações.

Permissões de diretório

As permissões de acesso a diretórios são do tipo `d`. O significado das permissões individuais para diretórios é ligeiramente diferente.

Exemplo 27.2 *Exemplo de saída com permissões de diretórios*

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15  ProjectData
```

No Exemplo 27.2, "Exemplo de saída com permissões de diretórios" (p 416), o proprietário (`tux`) e o grupo proprietário (`project3`) do diretório `ProjectData` são fáceis de reconhecer. Ao contrário das permissões de acesso do arquivo em Acesso a arquivos (p 415), o conjunto de permissões de leitura (`r`) significa que o conteúdo do diretório pode ser mostrado. A permissão de gravação (`w`) significa que novos arquivos podem ser criados. A permissão executável (x) significa que o usuário pode mudar para esse diretório. No exemplo acima, o usuário `tux` e os membros do grupo `project3` podem mudar para o diretório `ProjectData` (`x`), exibir o seu conteúdo (`r`) e adicionar ou apagar arquivos (`w`). Por outro lado, os outros usuários recebem menos permissões de acesso. Eles podem digitar o diretório (`x`) e pesquisá-lo (`r`), mas não podem digitar novos arquivos (`w`).

27.2.2 Modificando permissões de arquivos

Mudando permissões de acesso

As permissões de acesso de um arquivo ou diretório podem ser mudadas pelo proprietário e, obviamente, pelo `root` com o comando `chmod` seguido dos parâmetros que mudam as permissões e os nomes de um ou mais arquivos. Os parâmetros formam categorias diferentes:

1. usuários interessados

- `u` (*usuário*) – proprietário do arquivo

- `g` (*grupo*) – grupo que possui o arquivo
- `o` (*outros*) – usuários adicionais (se nenhum parâmetro for informado, as mudanças se aplicarão a todas as categorias)

2. um caractere para apagamento (–), configuração (=) ou inserção (+)
3. as abreviações

- `r` - *ler*
- `w` - *gravar*
- `x` - *executar*

4. nome ou nomes de arquivos separados por espaços

Se, por exemplo, o usuário `tux` em Exemplo 27.2, “Exemplo de saída com permissões de diretórios” (p 416) também deseja conceder a outros usuários acesso de gravação (`w`) ao diretório `ProjectData`, ele pode fazer isso usando o comando `chmod o+w ProjectData`.

Entretanto, se ele quiser negar a todos os usuários, exceto a si mesmo, permissões de gravação, é possível fazer isso digitando o comando `chmod go-w ProjectData`. Para proibir todos os usuários de adicionarem um novo arquivo à pasta `ProjectData`, digite `chmod -w ProjectData`. Assim, nem mesmo o proprietário pode gravar o arquivo sem primeiro restabelecer as permissões de gravação.

Mudando permissões de propriedade

Outros comandos importantes para controlar a propriedade e as permissões dos componentes do sistema de arquivos são `chown` (mudar usuário) e `chgrp` (mudar grupo). O comando `chown` pode ser usado para transferir a propriedade de um arquivo para outro usuário. Entretanto, somente o `root` tem permissão para efetuar essa mudança.

Suponha que o arquivo `Roadmap` do Exemplo 27.2, “Exemplo de saída com permissões de diretórios” (p 416) não deva mais pertencer a `tux`, e sim ao usuário `geeko`. O `root` deverá digitar `chown geeko Roadmap`.

`chgrp` muda a propriedade do grupo do arquivo. Contudo, o proprietário do arquivo deve ser um membro do novo grupo. Dessa forma, o usuário `tux` do Exemplo 27.1, “Exemplo de saída com permissões de arquivos” (p 415) pode alternar o grupo que possui o arquivo `ProjectData` para `project4` com o comando `chgrp project4 ProjectData`, desde que ele seja membro desse novo grupo.

27.2.3 setuid Bit

Em determinadas situações, as permissões de acesso podem ser muito restritivas. No entanto, o Linux possui configurações adicionais para permitir a mudança temporária do usuário atual e da identidade do grupo para uma ação específica. Por exemplo, o programa `passwd` normalmente requer permissões de root para acessar `/etc/passwd`. Este arquivo contém algumas informações importantes, como os diretórios pessoais de usuários e IDs de usuário e grupo. Sendo assim, um usuário normal não poderia mudar `passwd`, já que seria muito arriscado conceder a todos os usuários acesso direto a este arquivo. Uma possível solução para esse problema é o mecanismo *setuid*. O setuid (definir ID do usuário) é um atributo de arquivo especial que instrui o sistema a executar programas marcados adequadamente com um ID de usuário específico. Considere o comando `passwd`:

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Você pode ver o `s` que denota que setuid bit está definido para a permissão do usuário. Por meio do setuid bit, todos os usuários iniciando o comando `passwd` o executam como `root`.

27.2.4 setgid Bit

O setuid bit se aplica a usuários. Entretanto, existe também uma propriedade equivalente para grupos: o *setgid* bit. Um programa para o qual esse bit foi definido é executado com o ID do grupo no qual ele foi gravado, independentemente do usuário que iniciou o programa. No entanto, em um diretório com o setgid bit, todos os arquivos e diretórios criados recentemente são atribuídos ao grupo ao qual o diretório pertence. Considere o seguinte diretório de exemplo:

```
drwxrws--- 2 tux archive 48 Nov 19 17:12
  backup
```

Você pode ver o `s` que denota que o setuid bit está definido para a permissão do usuário. O proprietário do diretório e membros do grupo `archive` poderão acessar este diretório. Os usuários que não são membros deste grupo são "mapeados" para o grupo respectivo. O ID de grupo efetivo de todos os arquivos gravados será `archive`. Por exemplo, um programa de backup que é executado com o ID de grupo `archive` é capaz de acessar este diretório mesmo sem privilégios de root.

27.2.5 Sticky Bit

Também existe o *sticky bit*. Existe uma diferença caso ele pertença a um programa executável ou a um diretório. Se ele pertencer a um programa, qualquer arquivo marcado dessa forma será carregado na memória RAM a fim de evitar a necessidade de obtê-lo no disco rígido toda vez que for usado. Esse atributo é usado raramente, pois os discos rígidos modernos são muito rápidos. Se este bit estiver designado a um diretório, ele impedirá que usuários apaguem arquivos de outros usuários. Exemplos típicos incluem os diretórios `/tmp` e `/var/tmp`:

```
drwxrwxrwt   2 root  root   1160 2002-11-19 17:15 /tmp
```

27.2.6 Listas de controle de acesso

O conceito de permissão tradicional para objetos do sistema de arquivos do Linux, como arquivos ou diretórios, pode ser expandido com o uso de ACLs. Elas admitem a atribuição de permissões a usuários individuais ou a grupos que não sejam o proprietário original ou a um grupo proprietário de um objeto do sistema de arquivos.

Arquivos ou diretórios com permissões de acesso estendidas podem ser detectados com um simples comando `ls -l`:

```
-rw-r--r--+ 1 tux project3 14197 Jun 21  15:03 Roadmap
```

O proprietário do `Roadmap` é o `tux` que pertence ao grupo `project3`. O `tux` contém acesso de gravação e leitura a este arquivo. O grupo e todos os usuários têm acesso de leitura. A única diferença que diferencia esse arquivo de um arquivo sem uma ACL é o + extra na primeira coluna com os bits de permissão.

Obtenha detalhes sobre a ACL executando `getfacl Roadmap`:

```
# file:  Roadmap
# owner: tux
# group: project3
```

```
user::rw-
user:jane:rw-       effective: r--
group::r--
group:djungle:rw-   effective: r--
mask::r--
other::---
```

As três primeiras linhas da saída não retêm informações que não estejam disponíveis com `ls -l`. Essas linhas informam somente o nome do arquivo, o proprietário e o grupo proprietário. As linhas de 4 a 9 contêm as entradas de ACL. As permissões de acesso convencional representam um subconjunto das possíveis permissões quando se usa ACLs. A ACL do exemplo concede acesso de leitura e gravação ao proprietário do arquivo, assim como ao usuário `jane` (linhas 4 e 5). O conceito convencional foi expandido permitindo o acesso a um usuário extra. O mesmo se aplica ao acesso de grupo. O grupo proprietário possui permissões de leitura (linha 6) e o grupo `djungle` possui permissões de leitura e gravação. A entrada `mask` na linha 8 reduz as permissões efetivas para o usuário `jane` e o grupo `djungle` para acesso de leitura. Outros usuários e grupos não recebem nenhum tipo de acesso ao arquivo (linha 9).

Foram fornecidas apenas informações básicas. Encontre mais informações detalhadas sobre ACLs no Capítulo 24, *Listas de controle de acesso no Linux* (p 365).

27.3 Comandos importantes do Linux

Esta seção oferece uma visão geral dos comandos mais importantes do sistema SUSE LINUX. Existem muitos comandos além dos relacionados neste capítulo. Junto com os comandos individuais, são relacionados parâmetros e, quando apropriado, é apresentado o exemplo de um típico aplicativo. Para saber mais sobre os vários comandos, use as páginas de manual, acessadas com `man` seguidas pelo nome do comando, por exemplo, `man ls`.

Nas páginas de manual, desloque-se para cima e para baixo com PgUp e PgDn. Desloque-se entre o início e o fim do documento com Home e End. Conclua esta exibição pressionando Q. Aprenda mais sobre o próprio comando `man` com `man man`.

Na visão geral a seguir, os elementos do comando individual são gravados em estilos de fonte diferentes. O comando e suas opções obrigatórias são sempre impressos como

`opç o de comando`. Especificações ou parâmetros que não são necessários estão localizados entre `[colchetes]`.

Ajuste as configurações de acordo com as suas necessidades. Não faz sentido escrever `ls file` se não há um arquivo chamado `file`. Geralmente, você pode combinar vários parâmetros, por exemplo, escrevendo `ls –la` em vez de `ls –l –a`.

27.3.1 Comandos de arquivo

A seção a seguir lista os comandos mais importantes para o gerenciamento de arquivos. Ela abrange desde a administração geral dos arquivos até a manipulação das ACLs (Access Control Lists - Listas de Controle de Acesso) do sistema de arquivos.

Administração de arquivos

`ls [options] [files]`

Se você executar o comando `ls` sem nenhum parâmetro adicional, o programa relacionará resumidamente o conteúdo do diretório atual.

`–l`
Lista detalhada

`–a`
Exibe arquivos ocultos

`cp [options] source target`

Copia `source` para `target`.

`-i`
Aguarda a confirmação, se necessário, antes que um `target` seja sobrescrito

`-r`
Copia recursivamente (inclui subdiretórios)

`mv [options] source target`

Copia `source` para `target` e depois apaga o `source` original.

-b
Cria uma cópia de backup do `source` antes do deslocamento

-i
Aguarda a confirmação, se necessário, antes que um `targetfile` seja sobrescrito

`rm [options] files`

Remove os arquivos especificados do sistema de arquivos. Os diretórios não são removidos por `rm`, a menos que a opção `-r` seja usada.

`-r`
Apaga subdiretórios existentes

`-i`
Aguarda confirmação antes de apagar cada arquivo.

`ln [options] source target`

Cria um link interno do `source` para o `target`. Normalmente, um link como esse aponta diretamente para o `source` no mesmo sistema de arquivos. Entretanto, se `ln` for executado com a opção `-s`, ele criará um link simbólico que apontará apenas para o diretório no qual o `source` está localizado, permitindo vincular sistemas de arquivos.

-s
Cria um link simbólico

`cd [options] [directory]`

Muda o diretório atual. O comando `cd` sem parâmetros muda para o diretório pessoal do usuário.

`mkdir [options] directory`

Cria um novo diretório.

`rmdir [options] directory`

Apaga o diretório especificado, se ele já estiver vazio.

chown [options] username[:[group]] files

Transfere a propriedade de um arquivo para o usuário com o nome de usuário especificado.

-R
Muda arquivos e diretórios em todos os subdiretórios

chgrp [options] groupname files

Transfere a propriedade do grupo de determinado `file` para o grupo com o nome especificado. O proprietário do arquivo só pode mudar a propriedade do grupo se for membro tanto do grupo atual quanto do novo grupo.

chmod [options] mode files

Muda as permissões de acesso.

O parâmetro `mode` tem três partes: `group`, `access` e `access type`. `group` aceita os seguintes caracteres:

u
user

g
group

o
others

Usando `access`, conceda acesso com o comando + e negue-o com –.

O `access type` é controlado pelas seguintes opções:

r
read

w
write

x
execute – executando arquivos ou mudando para o diretório.

s

Setuid bit – o aplicativo ou programa é iniciado como se ele tivesse sido inicializado pelo proprietário do arquivo

Uma opção é usar um código numérico. Os quatro dígitos desse código são compostos pela soma dos valores 4, 2 e 1 – o resultado decimal de uma máscara binária. O primeiro dígito define o set user ID (SUID) (4), o set group ID (2) e os bits sticky (1). O segundo dígito define as permissões do proprietário do arquivo. O terceiro dígito define as permissões dos membros do grupo e o último define as permissões para todos os usuários. A permissão de leitura é definida com 4, a permissão de gravação com 2 e a permissão para execução de um arquivo com 1. O proprietário do arquivo recebe um 6 ou 7 para arquivos executáveis.

`gzip [parameters] files`

Este programa compacta o conteúdo dos arquivos usando algoritmos matemáticos complexos. Os arquivos compactados dessa forma recebem a extensão `.gz` e precisam ser descompactados antes de serem usados. Para compactar vários arquivos ou até mesmo diretórios inteiros, use o comando `tar`.

-d

Descompacta os arquivos gzip compactados para que eles retornem ao seu tamanho original e possam ser processados normalmente (como o comando `gunzip`)

`tar options archive files`

`tar` coloca um ou mais arquivos em um arquivo. A compactação é opcional. O comando `tar` é razoavelmente complexo, com algumas opções disponíveis. As opções usadas mais freqüentemente são:

-f

Grava a saída em um arquivo, e não na tela, como geralmente é o caso

-c

Cria um novo arquivo tar

-r

Adiciona arquivos a um arquivo existente

-t
Apresenta a saída do conteúdo de um arquivo

-u
Adiciona arquivos, mas somente se eles forem mais novos que os arquivos já existentes no arquivo

-x
Descompacta arquivos de um arquivo (*extração*)

-z
Compacta o arquivo resultante com `gzip`

-j
Compacta o arquivo resultante com `bzip2`

-v
Relaciona os arquivos processados

Os arquivos criados pelo comando `tar` terminam com `.tar`. Se o arquivo tar também tiver sido compactado com o comando `gzip`, a extensão será `.tgz` ou `.tar.gz`. Se ele tiver sido compactado com o comando `bzip2`, a extensão será `.tar.bz2`. Os exemplos de aplicativos podem ser encontrados em Seção 27.1.8, "Pacotes e compactação de dados" (p 412).

`locate patterns`

Este comando só estará disponível se você tiver instalado o pacote `findutils-locate`. O comando `locate` pode localizar o diretório em que um arquivo especificado se encontra. Se desejar, use curingas para especificar nomes de arquivo. O programa é muito rápido, pois usa um banco de dados especificamente criado para esse propósito (em vez de pesquisar todo o sistema de arquivos). Entretanto, esse fato também resulta em uma grande desvantagem: o comando locate é incapaz de localizar os arquivos criados após a última atualização do banco de dados. O banco de dados pode ser gerado por `root` com `updatedb`.

`updatedb [options]`

Este comando efetua uma atualização do banco de dados usado por `locate`. Para incluir arquivos em todos os diretórios existentes, execute o programa como `root`. Também é viável colocá-lo em segundo plano acrescentando um `&`; assim você

poderá continuar a trabalhar na mesma linha de comando (`updatedb &`). Esse comando geralmente é executado como uma tarefa cron diária (consulte `cron .daily`).

`find [options]`

Com `find`, procure um arquivo em determinado diretório. O primeiro argumento especifica o diretório no qual deve-se iniciar a pesquisa. A opção `-name` deve ser seguida por uma string de pesquisa que também pode incluir curingas. Diferentemente do comando `locate`, que usa um banco de dados, o `find` explora o diretório.

Comandos para acessar o conteúdo do arquivo

`cat [options] files`

O comando `cat` exibe o conteúdo de um arquivo imprimindo o conteúdo inteiro na tela, sem interrupção.

`-n`
Numera a saída na margem esquerda

`less [options] files`

Este comando pode ser usado para procurar o conteúdo do arquivo especificado. Role meia página para cima ou para baixo PgUp e PgDn ou uma página inteira para baixo com Space. Vá para o início ou fim do arquivo usando Home e End. Pressione Q para sair do programa.

`grep [options] searchstring files`

O comando grep procura uma string de pesquisa específica nos arquivos especificados. Se a string de pesquisa for encontrada, o comando exibirá a linha na qual `searchstring` foi encontrada com o nome do arquivo.

`-i`
Ignorar maiúsculas/minúsculas

`-H`
Exibe apenas os nomes dos respectivos arquivos, mas não as linhas de texto

-n
Adicionalmente, exibe os números das linhas nas quais encontrou uma ocorrência

-l
Relaciona apenas os arquivos nos quais `searchstring` não ocorre

diff [options] file1 file2

O comando `diff` compara o conteúdo de dois arquivos. A saída produzida pelo programa relaciona todas as linhas que não são correspondentes. Esse comando é freqüentemente usado por programadores que só precisam enviar suas alterações de programa, e não o código-fonte inteiro.

-q
Informa apenas se os dois arquivos são diferentes

-u
Produz um diff "unificado", que torna a saída mais legível

Sistemas de arquivos

mount [options] [device] mountpoint

Este comando pode ser usado para montar qualquer mídia de dados, como discos rígidos, unidades de CD-ROM e outras unidades, em um diretório do sistema de arquivos do Linux.

-r
montagem apenas leitura

-t filesystem
Especifica o sistema de arquivos; normalmente `ext2` para discos rígidos do Linux, `msdos` para mídia do MS-DOS, `vfat` para o sistema de arquivos do Windows e `iso9660` para CDs.

Para discos rígidos não definidos no arquivo `/etc/fstab`, também deve ser especificado o tipo de dispositivo. Nesse caso, apenas `root` pode montá-lo. Se o sistema de arquivos também tiver de ser montado por outros usuários, digite a opção `user` na linha adequada no arquivo `/etc/fstab` (separado por vírgulas) e grave essa mudança. Mais informações estão disponíveis na página de manual `mount(1)`.

umount [options] mountpoint

Este comando desmonta uma unidade montada no sistema de arquivos. Para evitar a perda de dados, execute o comando antes de retirar uma mídia de dados removível da sua unidade. Normalmente, apenas `root` tem permissão para executar os comandos `mount` e `umount`. Para permitir que outros usuários executem esses comandos, edite o arquivo `/etc/fstab` para especificar a opção `user` para a respectiva unidade.

27.3.2 Comandos do sistema

As seções a seguir relacionam alguns dos comandos mais importantes necessários para a recuperação de informações do sistema e o controle de rede e processos.

Informações do sistema

df [options] [directory]

O comando `df` (disk free), quando usado sem opções, exibe informações sobre o espaço total em disco, o espaço em disco atualmente em uso e o espaço livre em todos as unidades montadas. Se um diretório for especificado, as informações se limitarão à unidade na qual o diretório está localizado.

–h
Mostra o número de blocos ocupados em gigabytes, megabytes ou quilobytes – em formato legível

–T
Tipo do sistema de arquivos (ext2, nfs, etc.)

du [options] [path]

Este comando, quando executado sem nenhum parâmetro, mostra o espaço total em disco ocupado pelos arquivos e subdiretórios no diretório.

–a
Exibe o tamanho de cada arquivo individual

-h
Saída em forma legível

-s
Exibe apenas o tamanho total calculado

free [options]

O comando `free` exibe informações sobre o uso de RAM e de espaço de troca, mostrando a quantidade total e usada nas duas categorias. Consulte Seção 30.1.6, "O comando free" (p 482) para obter mais informações.

-b
Saída em bytes

-k
Saída em quilobytes

-m
Saída em megabytes

date [options]

Este simples programa exibe a hora atual do sistema. Se ele for executado como `root`, também poderá ser usado para mudar a hora do sistema. Detalhes sobre o programa estão disponíveis na página de manual date(1).

Processos

top [options]

`top` oferece uma visão geral rápida dos processos em execução. Pressione H para acessar uma página que explica resumidamente as opções principais para personalizar o programa.

ps [options] [process ID]
Se for executado sem opções, este comando exibirá uma tabela de todos os seus próprios programas ou processos – aqueles que você tiver iniciado. As opções para o comando não são precedidas de hífen.

aux
Exibe uma lista detalhada de todos os processos, independentemente do proprietário

`kill [options] process ID`

Infelizmente, às vezes, um programa não pode ser concluído de forma normal. Na maioria dos casos, você ainda poderá interromper um programa fora de controle ao executar o comando `kill`, especificando o ID do respectivo processo (consulte `top` e `ps`). O `kill` envia um sinal *TERM* que instrui o programa a se autodesligar. Se isso não ajudar, o seguinte parâmetro poderá ser usado:

-9
Envia um sinal *KILL* em vez de um sinal *TERM*, na maioria dos casos encerrando o processo especificado

`killall [options] processname`

Este comando assemelha-se ao `kill`, mas usa o nome do processo (em vez do ID do processo) como um argumento, eliminando todos os processos com esse nome.

Rede

`ping [options] hostname or IP address`

O comando `ping` é a ferramenta padrão usada para testar a funcionalidade básica das redes TCP/IP. Ele envia um pequeno pacote de dados para o host de destino solicitando uma resposta imediata. Se isso funcionar, o `ping` exibirá uma mensagem que indica que o link da rede está basicamente funcionando.

`-c number`
Determina o número total de pacotes a serem enviados e é concluído logo depois que os pacotes são despachados (por padrão, não há limitação definida).

`-f`
flood ping: envia o máximo possível de pacotes de dados; um método comum, reservado para `root` para o teste de redes

-i *value*
Especifica o intervalo entre dois pacotes de dados em segundos (padrão: um segundo)

nslookup

O sistema de nomes de domínio soluciona nomes de domínio para endereços IP. Com essa ferramenta, envie consultas para os servidores de nomes (servidores DNS).

telnet [options] hostname or IP address [port]
Na realidade, Telnet é um protocolo de Internet que permite trabalhar em hosts remotos de uma rede. Também é o nome de um programa do Linux que usa esse protocolo para habilitar operações em computadores remotos.

ATENÇÃO

Não use telnet em uma rede que esteja suscetível a "invasões" de terceiros. Especialmente na Internet, use os métodos de transferência criptografada, como `ssh`, para evitar que uma senha seja usada indevidamente (consulte a página de manual sobre `ssh`).

Diversos

passwd [options] [username]

Os usuários podem mudar suas próprias senhas, quando quiserem, com este comando. O administrador `root` pode usar o comando para mudar a senha de qualquer usuário no sistema.

su [options] [username]

O comando `su` possibilita o login com outro nome de usuário em uma sessão em execução. Especifique um nome de usuário e a senha correspondente. A senha não é necessária no `root`, pois o `root` é autorizado a assumir a identidade de qualquer usuário. Ao usar o comando sem especificar um nome de usuário, você deve informar a senha `root` e mudar o superusuário (`root`).

-
Use `su -` para iniciar um shell de login para o outro usuário.

`halt [options]`
Para evitar a perda de dados, você sempre deve usar esse programa para desligar o sistema.

`reboot [options]`

Faz o mesmo que `halt`, exceto que o sistema efetua uma reinicialização imediata.

`clear`

Este comando limpa a área visível do console. Não tem opções.

27.3.3 Mais informações

Existem muitos comandos além dos relacionados neste capítulo. Para obter informações sobre outros comandos ou obter informações mais detalhadas, é recomendável ler a publicação de O'Reilly, *Linux in a Nutshell*.

27.4 Editor vi

Os editores de texto ainda são usados por várias tarefas da administração do sistema como também para programação. No mundo do Unix, vi significa um editor que oferece funções de edição confortáveis e é mais ergonômico que muitos editores com suporte de mouse.

27.4.1 Modos de funcionamento

Basicamente, o vi tem três modos de funcionamento: modo *de inserção*, modo *de comando* e modo *estendido*. As chaves têm funções diferentes dependendo do modo. Na inicialização, o vi é normalmente definido para o modo *de comando*. A primeira coisa a aprender é como alternar entre os modos:

Modo de comando para Modo de inserção
Existem várias possibilidades, incluindo A para anexar, I para inserir ou O para uma nova linha sob a linha atual.

Modo de inserção para Modo de comando
Pressione Esc para sair do modo *de inserção*. O vi não pode ser terminado no modo *de inserção*, então é importante acostumar-se a pressionar Esc.

Modo de comando para Modo estendido
O modo *estendido* do vi pode ser ativado digitando-se dois-pontos (:). O modo *estendido* ou modo *ex* é semelhante a um editor independente orientado a linhas que pode ser usado para tarefas simples ou mais complexas.

Modo estendido para Modo de comando
Após executar um comando no modo *estendido*, o editor retorna automaticamente para o modo *de comando*. Se você decidir não executar nenhum comando no modo *estendido*, apague os dois-pontos com <—. O editor retorna para o modo *de comando*.

Não é possível alternar diretamente do modo *de inserção* para o modo *estendido* sem primeiro alternar para o modo *de comando*.

O vi, como outros editores, tem o seu próprio procedimento para terminar o programa. Você não pode terminar o vi enquanto estiver no modo *de inserção*. Primeiro, saia do modo *de inserção* pressionando Esc. Subseqüentemente, há duas opções:

1. *Sair sem gravar:* Para terminar o editor sem gravar as mudanças, digite : – Q – ! no modo *de comando*. O ponto de exclamação (!) faz com que o vi ignore quaisquer mudanças.

2. *Gravar e sair:* Existem várias possibilidades para gravar suas mudanças e terminar o editor. No modo *de comando*, use Shift + Z + Z. Para sair do programa e gravar todas as mudanças com o modo *estendido*, digite : – W – Q. No modo *estendido*, `w` corresponde a writ e `q` a quit.

27.4.2 vi em Ação

o vi pode ser usado como um editor normal. No modo *de inserção*, digite e apague texto com as teclas <— e Del. Use as teclas de seta para mover o cursor.

No entanto, estas teclas de controle geralmente causam problemas, porque existem vários tipos de terminais que usam códigos de tecla especiais. É aqui que o modo *de comando* entra em ação. Pressione Esc para alternar do modo *de inserção* para o modo

de comando. No modo *de comando*, mova o cursor com H, J, K e L. Essas teclas têm as seguintes funções:

H
: move um caractere para a esquerda

J
: move uma linha para baixo

K
: move uma linha para cima

L
: move um caractere para a direita

Os comandos no modo *de comando* permitem diversas variações. Para executar um comando várias vezes, simplesmente digite o número de repetições antes de digitar o comando real. Por exemplo, digite 5 L para mover o cursor cinco caracteres para a direita.

Uma seleção de comandos importantes é mostrada na Tabela 27.1, "Comandos simples do Editor vi" (p 434), mas esta lista ainda está bastante incompleta. Mais listas completas estão disponíveis na documentação encontrada na Seção 27.4.3, "Mais informações" (p 435)

Tabela 27.1 *Comandos simples do Editor vi*

Esc	Muda para o modo de comando
I	Muda para o modo de inserção (caracteres aparecem na posição do cursor atual)
A	Muda para o modo de inserção (caracteres aparecem depois da posição do cursor atual)
Shift + A	Muda para o modo de inserção (caracteres são adicionados no fim da linha)
Shift + R	Muda para o modo de substituição (sobregrava o texto antigo)

R	Substitui o caractere sob o cursor
O	Muda para o modo de inserção (uma nova linha é inserida após a atual)
Shift + O	Muda para o modo de inserção (uma nova linha é inserida antes da atual)
X	Apaga o caractere atual
D – D	Apaga a linha atual
D – W	Apaga a palavra atual até o fim
C – W	Muda para o modo de inserção (o resto da palavra é sobregravado pelas próximas entradas do usuário)
U	Desfaz o último comando
Ctrl + R	Refaz a mudança que foi desfeita
Shift + J	Une a linha seguinte à linha atual
.	Repete o último comando

27.4.3 Mais informações

O vi suporta uma grande variedade de comandos. Ele permite o uso de macros, atalhos, buffers nomeados e vários outros recursos úteis. Uma descrição detalhada das várias opções excederia o escopo deste manual. O SUSE Linux é fornecido com vim (vi aperfeiçoado), uma versão melhorada do vi. Existem diversas fontes de informações para este aplicativo:

- vimtutor é um tutor interativo para vim.
- No vim, digite o comando `:help` para obter ajuda sobre várias questões.

- Um manual sobre o vim está disponível online em http://www.truth.sk/vim/vimbook-OPL.pdf.
- As páginas da Web do projeto vim em http://www.vim.org apresentam todos os tipos de notícias, listas de distribuição e outra documentação.
- Um número de fontes do vim estão disponíveis na Internet: http://www.selflinux.org/selflinux/html/vim.html, http://www.linuxgazette.com/node/view/9039 e http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html. Consulte http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html para obter mais links a tutoriais.

IMPORTANTE: A Licença do VIM

O vim é "software para caridade" o que significa que os autores não cobram pelo software mas o encorajam a suportar um projeto sem fins lucrativos com uma contribuição monetária. Este projeto solicita ajuda para crianças pobres na Uganda. Há mais informações disponíveis online em http://iccf-holland.org/index.html, http://www.vim.org/iccf/ e http://www.iccf.nl/.

Inicializando e configurando um sistema Linux

28

A inicialização de um sistema Linux envolve vários componentes. Este capítulo descreve os princípios subjacentes e realça os componentes envolvidos, além de abordar o conceito de runlevels e a configuração do sistema SUSE com o`sysconfig`.

28.1 Processo de inicialização do Linux

O processo de inicialização do Linux consiste em vários estágios, e cada um deles é representado por outro componente. A lista a seguir resume o processo de inicialização e apresenta todos os principais componentes envolvidos.

1. **BIOS** Depois que o computador é desligado, o BIOS inicializa a tela e o teclado e testa a memória principal. Até esse estágio, a máquina não acessa nenhuma mídia de armazenamento em massa. Em seguida, as informações sobre a data e o horário atuais e sobre os periféricos mais importantes são carregadas dos valores do CMOS. Quando o primeiro disco rígido e sua geometria são reconhecidos, o controle do sistema passa do BIOS para o carregador de boot.

2. **Carregador de boot** O primeiro setor de dados físico de 512 bytes do primeiro disco rígido é carregado na memória principal e o *carregador de boot* existente no início desse setor assume o controle. Os comandos executados pelo carregador de boot determinam a parte restante do processo de boot. Desse modo, os primeiros 512 bytes do primeiro disco rígido são chamados de MBR *(Master Boot Record - Registro Mestre de Inicialização)*. O carregador de boot passa o

controle para o sistema operacional real, nesse caso, o kernel Linux. Mais informações sobre o GRUB, o carregador de boot do Linux, podem ser encontradas no Capítulo 29, *O Carregador de Boot* (p 453).

3. **Kernel e initramfs** Para passar o controle do sistema, o carregador de boot carrega na memória o kernel e um sistema de arquivos inicial baseado em RAM (initramfs). O conteúdo do ramfs inicial pode ser usado diretamente pelo kernel. O init ramfs contém um pequeno executável chamado init que realiza a montagem do sistema de arquivos raiz. Em versões anteriores do SUSE Linux, essas tarefas eram realizadas pelo initrd e linuxrc, respectivamente. Para obter mais informações sobre o initramfs, consulte a Seção 28.1.1, “initramfs” (p 438).

4. **init no initramfs** Este programa executa todas as ações necessárias para montar o sistema de arquivos raiz adequado, por exemplo, fornecer a funcionalidade de kernel para o sistema de arquivos e os drivers de dispositivo necessários aos controladores de armazenamento em massa. Uma vez encontrado o sistema de arquivos raiz, ele é verificado quanto a erros e montado. Se esse procedimento for bem-sucedido, o initramfs será limpo e o programa init no sistema de arquivos raiz será executado. Para obter mais informações sobre o init, consulte a Seção 28.1.2, “init no initramfs” (p 439).

5. **init** O init realiza a inicialização do sistema através de diversos níveis, oferecendo funcionalidades diferentes. Ele é descrito na Seção 28.2, “O processo init” (p 441).

28.1.1 initramfs

initramfs é um pequeno sistema de arquivos que pode ser carregado pelo kernel em um disco RAM. Ele fornece um ambiente Linux mínimo que permite a execução de programas antes da montagem do sistema de arquivos raiz. Esse ambiente é carregado na memória pelas rotinas de BIOS e não têm requisitos de hardware específicos, além de memória suficiente. O initramfs deve sempre fornecer um executável chamado init que deve executar o programa init no sistema de arquivos raiz para a continuação do processo de boot.

Antes da montagem do sistema de arquivos raiz e a inicialização do sistema operacional, o kernel precisa dos drivers correspondentes para acessar o dispositivo em que o sistema de arquivos raiz está localizado. Esses drivers podem incluir drivers especiais para determinados tipos de unidades de disco rígido ou até drivers de rede para acesso a um

sistema de arquivos de rede. Os módulos necessários para o sistema de arquivos raiz podem ser carregados pelo init no initramfs. O initramfs está disponível durante todo o processo de boot. Assim, é possível manipular todos os eventos hotplug gerados durante o boot.

Se você precisar mudar o hardware (discos rígidos) em um sistema instalado e esse hardware necessitar da existência de diversos drivers no kernel durante o boot, será necessário atualizar o initramfs. Para isso, basta chamar o `mkinitrd`, o que também era feito no initrd, predecessor do initramfs. A chamada de `mkinitrd` sem argumentos cria um initramfs. A chamada de `mkinitrd -R` cria um initrd. No SUSE Linux, os módulos a serem carregados são especificados pela variável `INITRD_MODULES` em `/etc/sysconfig/kernel`. Após a instalação, essa variável é definida automaticamente com o valor correto. Os módulos são carregados na mesma ordem em que são exibidos em `INITRD_MODULES`. Isso será especialmente importante se vários drivers SCSI forem usados, pois, caso contrário, os nomes dos discos rígidos seriam mudados. Em suma, seria suficiente apenas carregar os drivers necessários para acessar o sistema de arquivos raiz. Contudo, todos os drivers SCSI necessários à instalação são carregados por meio do initramfs ou initrd porque o carregamento posterior poderia ser problemático.

IMPORTANTE: Atualizando o initramfs ou o initrd

O carregador de boot carrega o initramfs ou initrd da mesma maneira que o kernel. Não é necessário reinstalar o GRUB após a atualização do initramfs ou initrd, pois o GRUB procura o arquivo correto no diretório durante a inicialização.

28.1.2 init no initramfs

O principal objetivo do init no initramfs é preparar a montagem do sistema de arquivos raiz e o acesso a este. Dependendo da configuração do sistema, o init é responsável pelas tarefas a seguir.

Carregamento de módulos Kernel
: Dependendo da configuração do seu hardware, drivers especiais podem ser necessários para acessar os componentes de hardware do computador (sendo que o componente mais importante é a unidade de disco rígido). Para acessar o sistema

de arquivos raiz final, o kernel precisa carregar os drivers adequados do sistema de arquivos.

Gerenciamento de configurações RAID e LVM
Se você tiver configurado o sistema para armazenar o sistema de arquivos raiz na RAID ou LVM, o init configurará a LVM ou a RAID para permitir acesso posterior ao sistema de arquivos raiz. Informações sobre a RAID podem ser encontradas na Seção 2.3, “Configuração de RAID de software” (p 67). Informações sobre a LVM podem ser encontradas na Seção 2.2, “Configuração da LVM” (p 60).

Gerenciamento de conexões de rede
Se você tiver configurado o sistema para usar um sistema de arquivos raiz montado em rede (via NFS), o init deverá ter certeza de que os drivers de rede corretos foram carregados e de que estejam configurados para permitir acesso ao sistema de arquivos raiz.

Quando o init é chamado durante a primeira inicialização como parte do processo de instalação, suas tarefas são diferentes daquelas mencionadas anteriormente:

Localização da mídia de instalação
Quando o processo de instalação é iniciado, a máquina carrega um kernel de instalação e um initrd especial com o instalador do YaST proveniente da mídia de instalação. O instalador do YaST, que é executado em um sistema de arquivos RAM, precisa ter informações sobre a localização da mídia de instalação para acessá-la e instalar o sistema operacional.

Inicialização do reconhecimento de hardware e carregamento dos módulos kernel adequados
Como mencionado na Seção 28.1.1, “initramfs” (p 438), o processo de boot inicia com um conjunto mínimo de drivers que pode ser usado com a maioria das configurações de hardware. O init inicia um processo de exploração de hardware que determina o conjunto de drivers adequado para sua configuração de hardware. Esses valores são gravados posteriormente em `INITRD_MODULES` em `/etc/sysconfig/kernel` para que qualquer processo de boot subseqüente possa usar um initrd personalizado. Durante o processo de instalação, o init carrega esse conjunto de módulos.

Carregamento do sistema de instalação ou do sistema de recuperação
Depois que o hardware for reconhecido adequadamente e os drivers adequados forem carregados, o init iniciará o sistema de instalação, que contém o instalador do YaST ou o sistema de recuperação.

Inicialização do YaST
Por fim, o init inicia o YaST que, por sua vez, inicia a instalação do pacote e a configuração do sistema.

28.2 O processo init

O programa init é o processo de número 1. Ele é responsável pela inicialização do sistema da maneira necessária e, além disso, tem uma função especial. Ele é iniciado diretamente pelo kernel e resiste ao sinal 9, que normalmente elimina os processos. Todos os outros programas são iniciados diretamente pelo init ou por um de seus processos-filho.

O init é configurado centralmente no arquivo `/etc/inittab` em que os *runlevels* são definidos (consulte a Seção 28.2.1, “Runlevels” (p 441)). O arquivo também especifica os serviços e os daemons disponíveis em cada um dos níveis. Dependendo das entradas em `/etc/inittab`, vários scripts são executados pelo init. Para fins de clareza, esses scripts, chamados *scripts init*, residem no diretório `/etc/init.d` (consulte a Seção 28.2.2, “Scripts Init” (p 444)).

Todo o processo de inicialização e encerramento do sistema é mantido pelo init. Desse ponto de vista, o kernel pode ser considerado um processo em segundo plano cuja tarefa é manter todos os outros processos e ajustar o horário da CPU e o acesso ao hardware, de acordo com as solicitações de outros programas.

28.2.1 Runlevels

No Linux, os *runlevels* definem como o sistema é iniciado e quais serviços estão disponíveis no sistema em execução. Após a inicialização, o sistema é iniciado conforme definido em `/etc/inittab` na linha `initdefault`. Normalmente, é `3` ou `5`. Consulte a Tabela 28.1, “Runlevels disponíveis” (p 442). Como alternativa, é possível especificar o runlevel durante a inicialização (no prompt, por exemplo). Os parâmetros que não forem avaliados diretamente pelo próprio kernel serão passados para o init.

Tabela 28.1 *Runlevels disponíveis*

Runlevel	Descrição
0	Desligamento do sistema
S	Modo de usuário único; do prompt de inicialização, somente com mapeamento de teclado americano
1	Modo de usuário único
2	Modo multiusuário local sem rede remota (NFS, etc.)
3	Modo multiusuário completo com rede
4	Não usado
5	Modo multiusuário completo com rede e gerenciador de vídeo X — KDM, GDM ou XDM
6	Reinicialização do sistema

IMPORTANTE: Evite o Runlevel 2 com uma partição /usr montada via NFS

Você não deverá usar o runlevel 2 se seu sistema montar a partição `/usr` através do NFS. O diretório `/usr` mantém programas importantes, essenciais ao funcionamento adequado do sistema. Como o serviço NFS não está disponível no runlevel 2 (modo multiusuário local sem rede remota), o sistema seria seriamente restringido em muitos aspectos.

Para mudar os runlevels durante a execução do sistema, digite `init` e o número correspondente como um argumento. Somente o administrador do sistema pode fazer isso. A lista a seguir resume os comandos mais importantes na área de runlevel.

`init 1` ou `shutdown now`
O sistema muda para o *modo de usuário único*. Esse modo é usado para manutenção do sistema e tarefas de administração.

`init 3`
Todos os programas e serviços essenciais (incluindo a rede) são iniciados, e os usuários comuns podem efetuar login e trabalhar no sistema sem um ambiente gráfico.

`init 5`
O ambiente gráfico é habilitado. Ele pode ser uma das áreas de trabalho (GNOME ou KDE) ou qualquer gerenciador de janelas.

`init 0` ou `shutdown -h now`
O sistema é desligado.

`init 6` ou `shutdown -r now`
O sistema é desligado e, em seguida, reinicializado.

Runlevel `5` é o runlevel padrão em todas as instalações padrão do SUSE Linux. É solicitado o login dos usuários em uma interface gráfica. Se o runlevel padrão for `3`, o Sistema Windows X deverá ser configurado adequadamente, conforme descrito no Capítulo 35, *O sistema X Window* (p 545), antes que o runlevel seja alternado para `5`. Se isso for feito, verifique se o sistema funciona da maneira desejada, digitando `init 5`. Se tudo ocorrer conforme o esperado, você poderá usar o YaST para definir o runlevel padrão como `5`.

ATENÇÃO: Os erros em /etc/inittab podem resultar em uma falha de inicialização do sistema

Se `/etc/inittab` for danificado, o sistema poderá não ser inicializado adequadamente. Portanto, seja extremamente cuidadoso ao editar `/etc/inittab` e sempre mantenha um backup de uma versão intacta. Para reparar o dano, tente digitar `init=/bin/sh` após o nome do kernel no prompt de inicialização para inicializar diretamente em um shell. Depois disso, torne seu sistema de arquivos raiz gravável com o comando `mount -o remount,rw /` e substitua `/etc/inittab` pela versão de backup usando `cp`. Para impedir erros no sistema de arquivos, mude o sistema de arquivos raiz para somente leitura antes de reinicializar com `mount -o remount,ro /`.

Geralmente, há duas situações quando os runlevels são mudados. Primeiro, os scripts de parada do runlevel atual são iniciados, fechando alguns programas essenciais ao runlevel atual. Em seguida, os scripts do novo runlevel são iniciados. Na maioria dos

casos, vários programas são iniciados. Por exemplo, ocorre o seguinte quando o runlevel 3 muda para 5:

1. O administrador (`root`) solicita que o init mude para um runlevel diferente digitando `init 5`.

2. O init consulta seu arquivo de configuração (`/etc/inittab`) e determina se ele deve iniciar `/etc/init.d/rc` com o novo runlevel como parâmetro.

3. O `rc` chama todos os scripts de parada do runlevel atual, mas somente aqueles para os quais não há script de início no novo runlevel. Neste exemplo, todos os scripts residem em `/etc/init.d/rc3.d` (o runlevel antigo era 3) e iniciam com `K`. O número depois de `K` especifica a ordem de início, pois algumas dependências devem ser consideradas.

4. Os scripts do novo runlevel são os últimos a serem iniciados. Neste exemplo, eles estão em `/etc/init.d/rc5.d` e começam com `S`. O mesmo procedimento relativo à ordem em que eles foram iniciado se aplica nesse caso.

Ao mudar para o mesmo runlevel que o atual, o init somente verifica as mudanças em `/etc/inittab` e inicia as etapas adequadas, por exemplo, para iniciar um `getty` em outra interface.

28.2.2 Scripts Init

Há dois tipos de scripts em `/etc/init.d`:

Scripts executados diretamente pelo init
: Isso só ocorrerá durante o processo de boot ou se um encerramento imediato do sistema for iniciado (falha de energia ou pressionamento de Ctrl + Alt + Del). A execução desses scripts é definida em `/etc/inittab`.

Scripts executados indiretamente pelo init
: São executados durante a mudança do runlevel e sempre chamam o script master `/etc/init.d/rc`, que garante a ordem correta dos scripts relevantes.

Todos os scripts estão localizados em `/etc/init.d`. Os scripts para mudança do runlevel também são encontrados nesse local, mas são chamados através de links simbólicos em um dos subdiretórios (`/etc/init.d/rc0.d` para `/etc/init.d/`

rc6.d). Isso só serve para fins de clareza, além de evitar scripts duplicados se forem usados em vários runlevels. Como todos os scripts podem ser executados como de início ou de parada, eles devem entender os parâmetros `start` e `stop`. Os scripts também entendem as opções `restart`, `reload`, `force-reload` e `status`. Essas diversas opções são explicadas na Tabela 28.2, "Opções possíveis do script init" (p 445). Os scripts executados diretamente pelo init não têm esses links. Eles são executados independentemente do runlevel, quando necessário.

Tabela 28.2 *Opções possíveis do script init*

Opção	Descrição
`start`	Inicia o serviço.
`stop`	Pára o serviço.
`restart`	Se o serviço estiver sendo executado, o pára e o reinicia. Se não estiver, o inicia.
`reload`	Recarrega a configuração sem parar e reiniciar o serviço.
`force-reload`	Recarrega a configuração se o serviço suportá-la. Caso contrário, age como se `restart` tivesse sido ativado.
`status`	Mostra o status atual do serviço.

Os links em cada subdiretório específico de runlevel possibilitam a associação de scripts a diferentes runlevels. Durante a instalação ou desinstalação de pacotes, esses links são adicionados e removidos com a ajuda do programa insserv (ou usando `/usr/lib/lsb/install_initd`, que é um script que chama esse programa). Consulte a página de manual insserv(8) para obter detalhes.

Veja a seguir uma pequena apresentação dos scripts de boot e de parada iniciados primeiro e por último, respectivamente, bem como uma explicação do script de manutenção.

`boot`
: Executado na inicialização do sistema usando diretamente o init. É independente do runlevel escolhido e só é executado uma vez. Nesse momento, os sistemas de arquivos `proc` e `pts` são montados e o blogd (boot logging daemon) é ativado. Se

o sistema for inicializado pela primeira vez após uma atualização ou instalação, a configuração inicial do sistema será iniciada.

O daemon blogd é um serviço iniciado por boot e rc antes de qualquer outro. Ele será parado depois que os acionamentos feitos pelos scripts acima (por meio da execução de vários subscripts, por exemplo) forem concluídos. O blogd gravará a saída de tela no arquivo de registro `/var/log/boot.msg`, mas somente se e quando `/var` for montado para leitura-gravação. Caso contrário, o blogd armazenará no buffer todos os dados de tela até que `/var` se torne disponível. Obtenha mais informações sobre o blogd na página de manual blogd(8).

O script `boot` também é responsável pela inicialização de todos os scripts em `/etc/init.d/boot.d` com um nome iniciado com `S`. Nesse local, todos os sistemas de arquivos são verificados e os dispositivos de loop são configurados se necessário. O horário do sistema também é definido. Se ocorrer um erro durante a verificação e o reparo automáticos do sistema de arquivos, o administrador do sistema poderá intervir após digitar a senha raiz. Por fim, é executado o script `boot.local`.

`boot.local`
Digite aqui comandos adicionais a serem executados na inicialização antes de mudar para um runlevel. Ele pode ser comparado ao `AUTOEXEC.BAT` em sistemas DOS.

`boot.setup`
Este script é executado quando o modo de usuário único é mudado para outro runlevel e é responsável por várias configurações básicas, como o layout do teclado e a inicialização dos consoles virtuais.

`halt`
Este script é executado somente durante a mudança para o runlevel 0 ou 6. Ele é executado como `halt` ou `reboot`. O modo como `halt` é chamado determina se o sistema deve ser encerrado ou reinicializado.

`rc`
Este script chama os scripts de parada adequados do runlevel atual e os scripts de início do runlevel recém-selecionado.

Você pode criar seus próprios scripts e integrá-los facilmente no esquema descrito acima. Para obter instruções sobre como formatar, nomear e organizar scripts personalizados, consulte as especificações do LSB e as páginas de manual do `init`,

`init.d` e `insserv`. Além disso, consulte as páginas de manual do `startproc` e `killproc`.

ATENÇÃO: Scripts init defeituosos podem desligar o seu sistema

Scripts init defeituosos podem travar sua máquina. Edite esses scripts com muito cuidado e, se possível, submeta-os a testes detalhados no ambiente multiusuário. Algumas informações úteis sobre os scripts init podem ser encontradas na Seção 28.2.1, “Runlevels” (p 441).

Para criar um script init personalizado para determinado programa ou serviço, use o arquivo `/etc/init.d/skeleton` como gabarito. Grave uma cópia desse arquivo com o novo nome e edite o programa relevante e nomes de arquivos, caminhos e outros detalhes necessários. Você também pode precisar aprimorar o script com suas próprias partes, de modo que os acionamentos corretos sejam feitos pelo procedimento init.

O bloco `INIT INFO` na parte superior é uma parte necessária do script e deve ser editada. Consulte o Exemplo 28.1, “Um bloco INIT INFO mínimo” (p 447).

Exemplo 28.1 *Um bloco INIT INFO mínimo*

```
# BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Na primeira linha do bloco `INFO`, após `Provides:`, especifique o nome do programa ou serviço controlado pelo script init. Nas linhas `Required-Start:` e `Required-Stop:`, especifique todos os serviços que precisam ser iniciados ou parados antes de o próprio serviço ser iniciado ou parado. Essas informações são usadas posteriormente para gerar a numeração dos nomes de script, como encontrada nos diretórios de runlevel. Após `Default-Start:` e `Default-Stop:`, especifique os runlevels em que o serviço deve ser iniciado ou parado automaticamente. Por fim, para `Description:`, forneça uma breve descrição do serviço em questão.

Para criar os links dos diretórios de runlevel (`/etc/init.d/rc?.d/`) para os scripts correspondentes em `/etc/init.d/`, digite o comando `insserv` *`new-script-name`*. O programa insserv avalia o cabeçalho `INIT INFO` para criar

os links necessários para os scripts de início e parada nos diretórios de runlevel (`/etc/init.d/rc?.d/`). O programa também se encarrega da ordem correta de início e parada para cada runlevel, incluindo os números necessários nos nomes desses links. Se você preferir uma ferramenta gráfica para criar esses links, use o editor de runlevel fornecido pelo YaST, como descrito na Seção 28.2.3, “Configurando serviços do sistema (runlevel) com o YaST” (p 448).

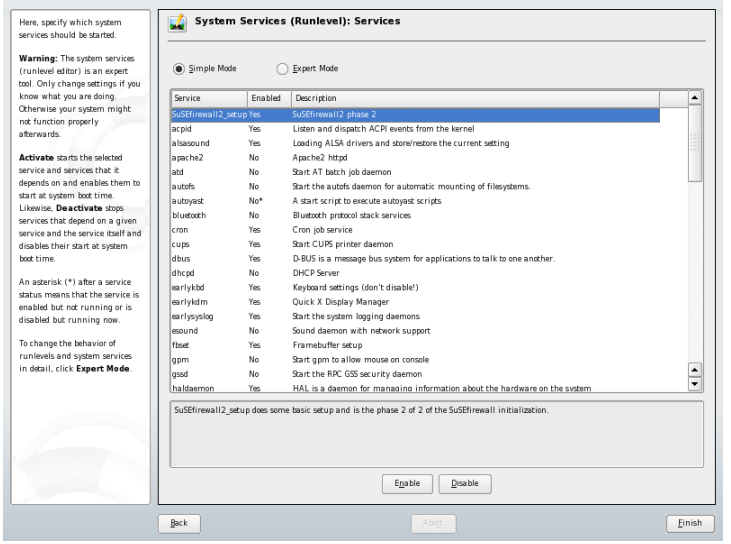
Se um script já existir em `/etc/init.d/`, deve ser integrado ao esquema de runlevel existente. Crie os links nos diretórios de runlevel imediatamente com insserv ou por meio do serviço correspondente no editor de runlevel do YaST. As mudanças serão aplicadas durante a próxima reinicialização, e o novo serviço será iniciado automaticamente.

Não defina esses links manualmente. Se houver algum erro no Bloco `INFO`, surgirão problemas quando `insserv` for executado posteriormente para algum outro serviço.

28.2.3 Configurando serviços do sistema (runlevel) com o YaST

Depois que o módulo YaST é iniciado com *YaST → Sistema → Serviços do Sistema (Runlevel)*, ele exibe uma visão geral que lista todos os serviços disponíveis e o status atual de cada um deles (desabilitado ou habilitado). Decida se o módulo deve ser usado no *Modo Simples* ou no *Modo de Especialista*. O *Modo Simples* padrão deve ser suficiente na maior parte dos casos. A coluna à esquerda mostra o nome do serviço, a coluna ao centro indica seu status atual e a coluna à direita fornece uma descrição resumida. Para o serviço selecionado, uma descrição mais detalhada é fornecida na parte inferior da janela. Para habilitar um serviço, selecione-o na tabela e, em seguida, selecione *Habilitar*. As mesmas etapas se aplicam para desabilitar um serviço.

Figura 28.1 *Serviços do Sistema (Runlevel)*


Here, specify which system services should be started.
Warning: The system services (runlevel editor) is an expert tool. Only change settings if you know what you are doing. Otherwise your system might not function properly afterwards.
Activate starts the selected service and services that it depends on and enables them to start at system boot time. Likewise, Deactivate stops services that depend on a given service and the service itself and disables their start at system boot time.
An asterisk (*) after a service status means that the service is enabled but not running or is disabled but running now.
To change the behavior of runlevels and system services in detail, click Expert Mode.
System Services (Runlevel): Services
Simple Mode
Expert Mode
Service
Enabled
Description
SuSEfirewall2_setup Yes SuSEfirewall2 phase 2
acpid Yes Listen and dispatch ACPI events from the kernel
alsasound Yes Loading ALSA drivers and store/restore the current setting
apache2 No Apache2 httpd
atd No Start AT batch job daemon
autofs No Start the autofs daemon for automatic mounting of filesystems.
autoyast No* A start script to execute autoyast scripts
bluetooth No Bluetooth protocol stack services
cron Yes Cron job service
cups Yes Start CUPS printer daemon
dbus Yes D-BUS is a message bus system for applications to talk to one another.
dhcpd No DHCP Server
earlykbd Yes Keyboard settings (don't disable!)
earlykdm Yes Quick X Display Manager
earlysyslog Yes Start the system logging daemons
esound No Sound daemon with network support
fbset Yes Framebuffer setup
gpm No Start gpm to allow mouse on console
gssd No Start the RPC GSS security daemon
haldaemon Yes HAL is a daemon for managing information about the hardware on the system
SuSEfirewall2_setup does some basic setup and is the phase 2 of 2 of the SuSEfirewall initialization.
Enable
Disable
Back
Abort
Finish

Para ter mais controle sobre os runlevels em que um serviço é iniciado ou parado ou para mudar o runlevel padrão, selecione primeiro *Modo de Especialista*. O runlevel padrão atual ou o "initdefault" (o runlevel em que o sistema é inicializado por padrão) é exibido na parte superior. Normalmente, o runlevel padrão de um sistema SUSE Linux é o 5 (modo multiusuário completo com rede e X). Uma alternativa adequada poderia ser o runlevel 3 (modo multiusuário completo com rede).

Esta caixa de diálogo do YaST permite a seleção de um dos runlevels (como listado na Tabela 28.1, "Runlevels disponíveis" (p 442)) como o novo padrão. Além disso, use a tabela mostrada nessa janela para habilitar ou desabilitar serviços e daemons individuais. A tabela lista os serviços e daemons disponíveis, mostra se eles estão habilitados no sistema e, se estiverem, para quais runlevels. Após selecionar uma das linhas com o mouse, clique nas caixas de seleção que representam os runlevels (*B*, *0*, *1*, *2*, *3*, *5*, *6* e *S*) para definir os runlevels em que o serviço ou daemon selecionado deve estar em execução. O runlevel 4 é inicialmente indefinido para permitir a criação de um runlevel personalizado. Uma breve descrição do serviço ou daemon selecionado no momento é fornecida abaixo da visão geral da tabela.

Com *Iniciar, Parar ou Atualizar*, decida se um serviço deve ser ativado. *Situação da Renovação* verifica o status atual. *Inicializar/Reinicializar* permite selecionar se você deseja aplicar as mudanças ao sistema ou restaurar as configurações existentes antes

da inicialização do editor de runlevel. A seleção de *Concluir* grava no disco as configurações mudadas.

ATENÇÃO: Configurações de runlevel defeituosas podem danificar o sistema

Configurações de runlevel defeituosas podem tornar um sistema inutilizável. Antes de aplicar as mudanças, tenha absoluta certeza sobre suas conseqüências.

28.3 Configuração do sistema via /etc/sysconfig

A configuração principal do SUSE Linux é controlada pelos arquivos de configuração em `/etc/sysconfig`. Os arquivos individuais em `/etc/sysconfig` são lidos somente pelos scripts para os quais são relevantes. Isso garante que as configurações de rede, por exemplo, somente precisem ser analisadas pelos scripts relacionados à rede. Muitos outros arquivos de configuração do sistema são gerados de acordo com as configurações em `/etc/sysconfig`. Essa tarefa é executada pelo SuSEconfig. Por exemplo, se você mudar a configuração da rede, o SuSEconfig também poderá fazer mudanças no arquivo `/etc/host.conf`, pois esse é um dos arquivos relevantes para a configuração da rede. Esse conceito permite realizar mudanças básicas na configuração sem a necessidade de reinicializar o sistema.

Há duas maneiras de editar a configuração do sistema. Use o Editor sysconfig do YaST ou edite manualmente os arquivos de configuração.

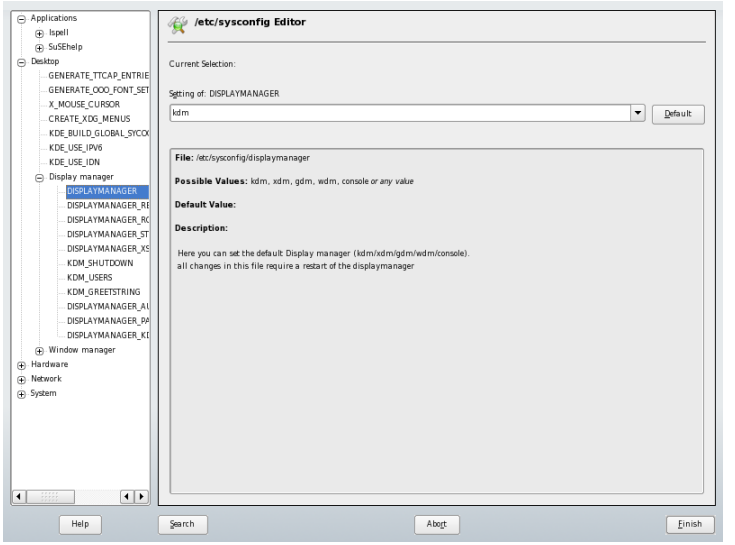
28.3.1 Mudando a configuração do sistema usando o Editor sysconfig do YaST

O editor sysconfig do YaST fornece um front end fácil de usar para a configuração do sistema. Sem conhecimento do local da variável de configuração que precisa ser mudada, você pode apenas usar a função de pesquisa interna desse módulo, mudar o valor dessa variável conforme o necessário, e permitir que o YaST se encarregue de aplicar essas mudanças, atualizando as configurações que dependem dos valores definidos no `sysconfig` e reiniciando os serviços.

ATENÇÃO: A modificação dos arquivos /etc/sysconfig/* pode danificar a instalação

Não modifique os arquivos `/etc/sysconfig` se você não tiver experiência e conhecimento prévios. Isso pode causar sérios danos ao sistema. Os arquivos em `/etc/sysconfig` contêm um pequeno comentário sobre cada variável para explicar seu efeito real.

Figura 28.2 *Configuração do sistema usando o Editor sysconfig*



A caixa de diálogo do Editor sysconfig do YaST é divida em três partes. A parte esquerda mostra uma tela de árvore de todas as variáveis configuráveis. Quando você seleciona uma variável, a parte direita exibe a seleção e a definição atuais dessa variável. Abaixo, uma terceira janela exibe uma pequena descrição da finalidade da variável, os valores possíveis, o valor padrão e o arquivo de configuração do qual essa variável se origina. A caixa de diálogo também fornece informações sobre qual script de configuração é executado após a mudança da variável e qual novo serviço é iniciado como resultado da mudança. O YaST solicita a confirmação das mudanças e informa quais scripts serão executados depois que você sair da caixa de diálogo selecionando *Concluir*. Além disso, selecione os serviços e scripts que devem ser ignorados agora e iniciados mais tarde. O YaST aplica todas as mudanças automaticamente e reinicia os serviços envolvidos para que elas sejam efetivadas.

28.3.2 Mudando manualmente a configuração do sistema

Para mudar manualmente a configuração do sistema, faça o seguinte

1. Torne-se `root`.
2. Coloque o sistema no modo de usuário único (runlevel 1) com `init 1`.
3. Mude os arquivos de configuração, conforme o necessário, com um editor de sua preferência.

   Se você não usar o YaST para mudar os arquivos de configuração em `/etc/sysconfig`, verifique se os valores das variáveis vazias estão representados por duas aspas (`KEYTABLE=""`) e se os valores com espaços em branco estão delimitados por aspas. Os valores constituídos de somente uma palavra não precisam ficar entre aspas.
4. Execute `SuSEconfig` para verificar se as mudanças foram efetivadas.
5. Coloque o sistema de volta no runlevel anterior com o comando `init` *`default_runlevel`*. Substitua *`runlevel_padrão`* pelo runlevel padrão do sistema. Escolha `5` para retornar ao modo multiusuário completo com rede e X ou escolha `3` se preferir trabalhar no modo multiusuário completo com rede.

Esse procedimento é relevante principalmente durante a mudança das configurações em todo o sistema, como a configuração da rede. Pequenas mudanças não devem requerer alternar para o modo de usuário único, mas você pode fazer isso para ter certeza de que todos os programas em questão foram reiniciados corretamente.

DICA: Definindo a configuração automatizada do sistema

Para desabilitar a configuração automatizada do sistema pelo SuSEconfig, defina a variável `ENABLE_SUSECONFIG` em `/etc/sysconfig/suseconfig` como `no`. Não desabilite o SuSEconfig se quiser usar o suporte de instalação do SUSE. Também é possível desabilitar parcialmente a configuração automática.

---

29 O Carregador de Boot

Este capítulo descreve como configurar o GRUB, o carregador de boot utilizado no SUSE Linux. Para realizar todas as configurações, há disponível um módulo especial YaST. Se você não estiver familiarizado com a idéia de entrar para o Linux, leia as seções a seguir para obter algumas informações de apoio. Este capítulo também descreve alguns problemas freqüentemente encontrados quando se inicializa com o GRUB e mostra as soluções para eles.

Este capítulo se concentra no gerenciamento de boot e na configuração do carregador de boot do GRUB. O procedimento de boot como um todo é detalhado em Capítulo 28, *Inicializando e configurando um sistema Linux* (p 437). O carregador de boot representa a interface entre a máquina (BIOS) e o sistema operacional (SUSE Linux). A configuração do carregador de boot influencia diretamente o boot do sistema operacional.

Os termos a seguir aparecem com freqüência neste capítulo e talvez precisem de alguma explicação:

Master boot record (registro mestre de boot)

A estrutura do MBR é definida por uma convenção que independe do sistema operacional. Os primeiros 446 bytes são reservados para o código do programa. Em geral, eles mantêm o programa do carregador de boot, neste caso, o GRUB. Os 64 bytes seguintes fornecem espaço para uma tabela de partição de até quatro entradas (consulte a seção “Tipos de partição” (Capítulo 1, *Instalação com o YaST*, ↑Inicialização)). A tabela de partição contém informações sobre o particionamento do disco rígido e sobre o tipo de sistema de arquivos. O sistema operacional precisa dessa tabela para lidar com o disco rígido. Os dois últimos bytes do MBR devem conter um “número mágico” estático (AA55). O MBR que contém um valor diferente

é registrado como inválido pela BIOS e por todos os sistemas operacionais que rodam em PCs.

Setores de boot

Os setores de boot são os primeiros setores das partições do disco rígido, com a execução da partição estendida, que serve meramente como "container" para outras partições. Esses setores de boot têm 512 bytes de espaço para o código usado para inicializar um sistema operacional instalado na partição respectiva. Isso se aplica aos setores de boot das partições formatadas do DOS, Windows e OS/2, que também contêm alguns dados básicos importantes do sistema de arquivos. Por outro lado, os setores de boot das partições do Linux estão inicialmente vazias depois de se configurar um sistema de arquivos. Portanto, uma partição do Linux *não é inicializável por si mesma*, mesmo que contenha um kernel e um sistema válido de arquivos raiz. Um setor de boot com código válido para inicializar o sistema tem o mesmo número mágico que o MBR em seus dois últimos bytes (`AA55`).

29.1 Gerenciamento de boot

No caso mais simples, ou seja, se houver apenas um sistema operacional instalado no computador, o gerenciamento de boot ocorre como descrito a seguir. Se houver vários sistemas operacionais instalados no computador, estão disponíveis as seguintes opções:

Inicializando sistemas adicionais a partir de mídias externas

Um dos sistemas operacionais pode ser inicializado do disco rígido. Os outros sistemas operacionais são inicializados através de um gerenciador de boot instalado em uma mídia externa (disquete, CD, mídia de armazenamento USB).

Instalando um gerenciador de boot no MBR

O gerenciador de boot permite a instalação simultânea e o uso alternado de vários sistemas em um computador. Os usuários podem selecionar o sistema a ser inicializado durante o processo de boot. Para escolher outro sistema, o computador deve ser reinicializado. Isso só é possível se o gerenciador de boot selecionado for compatível com os sistemas operacionais instalados. GRUB, o gerenciador de boot usado no SUSE Linux.

29.2 Selecionando um carregador de boot

Por padrão, o carregador de boot GRUB é usado no SUSE Linux. No entanto, em alguns casos e para grupos especiais de hardwares e softwares, o LILO pode ser mais adequado. Se você atualizar uma versão mais antiga do SUSE Linux que usa LILO, este é instalado.

No Banco de Dados de Suporte, na palavra-chave LILO e em `/usr/share/doc/packages/lilo`, há informações disponíveis sobre a instalação e a configuração do LILO.

29.3 Inicializando com o GRUB

O GRUB (Grand Unified Bootloader) compreende dois estágios: o stage1 consiste em 512 bytes e é gravado no MBR ou no setor de boot da partição de um disco rígido ou de um disquete. Depois disso, o stage2 é carregado. Este estágio contém o código real do programa. A única tarefa do primeiro estágio é carregar o segundo estágio do carregador de boot.

O stage2 consegue acessar os sistemas de arquivos. Atualmente, são suportados o Ext2, Ext3, ReiserFS, Minix e o sistema de arquivos FAT do DOS usado pelo Windows. Até certo ponto, JFS, XFS, e UFS e FFS usados pelos sistemas BSD também são suportados. Desde a versão 0.95, o GRUB também pode ser inicializado de um CD ou DVD que contenha um sistema de arquivos padrão ISO 9660 que está de acordo com a especificação “El Torito”. Mesmo antes de o sistema ser inicializado, o GRUB pode acessar os sistemas de arquivos dos dispositivos de disco BIOS suportados (disquetes ou discos rígidos, unidades de CD e unidades de DVD detectadas pelo BIOS). Portanto, as alterações realizadas no arquivo de configuração do GRUB (`menu.lst`) não exigem a reinstalação do gerenciador de boot. Quando o sistema é inicializado, o GRUB carrega o arquivo de menu com os caminhos e dados de partição válidos do kernel ou do disco RAM inicial (`initrd`) e localiza os arquivos.

A configuração atual do GRUB se baseia em três arquivos que são descritos a seguir:

/boot/grub/menu.lst

Este arquivo contém todas as informações sobre partições ou sistemas operacionais que podem ser inicializados com o GRUB. Sem essas informações, o controle de sistema não pode ser passado para o sistema operacional.

/boot/grub/device.map

Esse arquivo traduz os nomes dos dispositivos da notação do GRUB e do BIOS para os nomes de dispositivos do Linux.

/etc/grub.conf

Esse arquivo contém os parâmetros e as opções que o shell do GRUB precisa para instalar corretamente o carregador de boot.

O GRUB pode ser controlado de várias maneiras. As entradas de boot de uma configuração existente podem ser selecionadas no menu gráfico (tela de apresentação). A configuração é carregada a partir do arquivo `menu.lst`.

No GRUB, todos os parâmetros de boot podem ser alterados antes do boot. Por exemplo, os erros cometidos durante a edição do arquivo de menu podem ser corrigidos desta maneira. Os comandos de boot também podem ser inseridos de forma interativa através de um tipo de prompt de entrada (consulte o item "Editando as entradas de menu durante o procedimento de boot" (p 461)). O GRUB oferece a possibilidade de determinar a localização do kernel e do `initrd` antes do boot. Dessa maneira, você pode até inicializar um sistema operacional instalado para o qual não existe entrada na configuração do carregador de boot.

O *shell do GRUB* fornece uma emulação do GRUB no sistema instalado. Ele pode ser usado para instalar o GRUB ou testar novas configurações antes de aplicá-las. Consulte o item Seção 29.3.4, "O shell do GRUB" (p 464).

29.3.1 O menu de boot do GRUB

A tela de apresentação gráfica com o menu de boot baseia-se no arquivo de configuração do GRUB `/boot/grub/menu.lst`, que contém todas as informações sobre todas as partições ou sistemas operacionais que podem ser inicializados pelo menu.

Todas as vezes em que o sistema é inicializado, o GRUB carrega o arquivo de menu a partir do sistema de arquivos. Por essa razão, o GRUB não precisa ser reinstalado depois de todas as modificações no arquivo. Use o carregador de boot YaST para modificar a configuração do GRUB conforme descrito no Seção 29.4, “Configurando o carregador de boot com o YaST” (p 466).

O arquivo de menu contém comandos. A sintaxe é muito simples. Cada linha contém um comando seguido de parâmetros opcionais separados por espaços, como ocorre no shell. Por razões históricas, alguns comandos admitem um = na frente do primeiro parâmetro. Os comentários são introduzidos por um hash (#).

Para identificar os itens do menu na visão geral do menu, especifique um `título` para cada entrada. O texto (incluindo os espaços) que vem depois da palavra-chave `título` é exibido como opção selecionável no menu. Todos os comandos até o próximo `título` são executados quando se seleciona esse item de menu.

O caso mais simples é o redirecionamento para os carregadores de boot de outros sistemas operacionais. O comando é `chainloader`, e o argumento é geralmente o bloco de boot de outra partição na notação do bloco do GRUB. Por exemplo:

```
chainloader (hd0,3)+1
```

Os nomes de dispositivo no GRUB são explicados em “Convenções de nomenclatura para discos rígidos e partições” (p 458). O exemplo apresentado especifica o primeiro bloco da quarta partição do primeiro disco rígido.

Use o comando `kernel` para especificar uma imagem do kernel. O primeiro argumento é o caminho para a imagem do kernel em uma partição. Os outros argumentos são passados para o kernel na linha de comando.

Se o kernel não contiver drivers incorporados para acesso à partição raiz, o `initrd` deve ser especificado com um comando separado do GRUB cujo único argumento é o caminho para o arquivo `initrd`. Como o endereço de carregamento do `initrd` é gravado na imagem do kernel carregado, o comando `initrd` deve vir imediatamente após o comando `kernel`.

O comando `root` simplifica a especificação do kernel e dos arquivos initrd. O único argumento de `root` é um dispositivo do GRUB ou uma partição em um dispositivo do GRUB. Esse dispositivo é usado para todos os kernels, `initrd`, ou para outros caminhos de arquivo para os quais não há dispositivos explicitamente especificados

até o próximo comando `root`. Esse comando não é usado no arquivo `menu.lst` gerado durante a instalação. Ele apenas facilita a edição manual.

O comando `boot` está implícito no fim de cada entrada do menu, assim ele não precisa ser gravado no arquivo de menu. No entanto, para usar o GRUB interativamente para o boot, você deve inserir o comando `boot` no final. O comando em si não tem argumentos. Ele meramente inicializa a imagem do kernel carregado ou do carregador de cadeia especificado.

Depois de gravar todas as entradas de menu, defina uma delas como entrada `default`. Do contrário, é utilizada a primeira (entrada `0`). Você também pode especificar um tempo de espera em segundos depois do qual a entrada default deve ser inicializada. `timeout` e `default` geralmente precedem as entradas de menu. Um arquivo de exemplo é descrito em "Um exemplo de arquivo de menu" (p 459).

Convenções de nomenclatura para discos rígidos e partições

As convenções de nomenclatura que o GRUB utiliza para discos rígidos e partições diferem daquelas usadas para os dispositivos normais do LINUX. No GRUB, a numeração das partições começa no zero. Assim, (`hd0,0`) é a primeira partição do primeiro disco rígido. Em uma máquina desktop comum, com um disco rígido conectado como master principal, o nome do dispositivo correspondente no Linux é `/dev/hda1`.

As quatro partições principais possíveis são atribuídas aos números de partição de `0` a `3`. As partições lógicas são numeradas a partir de `4`:

```
(hd0,0)    primeira partiç o prim ria do primeiro disco rígido
(hd0,1)    segunda partiç o prim ria
(hd0,2)    terceira partiç o prim ria
(hd0,3)    quarta partiç o prim ria (em geral uma partiç o estendida)
(hd0,4)    primeira partiç o lógica
(hd0,5)    segunda partiç o lógica
```

O GRUB não faz distinção entre os dispositivos IDE, SCSI e RAID. Todos os discos rígidos reconhecidos pelo BIOS ou por outras controladoras são numerados de acordo com a seqüência de boot predefinido no BIOS.

Infelizmente, o GRUB não consegue mapear os nomes dos dispositivos do Linux exatamente para os nomes dos dispositivos da BIOS. Ele gera esse mapeamento com a ajuda de um algoritmo e o salva no arquivo`device.map`, que pode ser editado se

necessário. Em Seção 29.3.2, “O arquivo device.map” (p 462), há informações sobre o arquivo `device.map`.

O caminho completo do GRUB consiste em um nome de dispositivo escrito entre parênteses e no caminho para o arquivo no sistema de arquivos na partição especificada. O caminho começa com uma barra. Por exemplo, o kernel inicializável poderia ser especificado como segue em um sistema com um disco rígido único de IDE que contém o Linux em sua primeira partição:

```
(hd0,0)/boot/vmlinuz
```

Um exemplo de arquivo de menu

O exemplo a seguir mostra a estrutura de um arquivo de menu do GRUB. A instalação de exemplo compreende uma partição de boot do Linux em `/dev/hda5`, uma partição raiz em `/dev/hda7` e uma instalação do Windows em `/dev/hda1`.

```
ggfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd

title windows
   chainloader(hd0,0)+1

title floppy
   chainloader(fd0)+1

title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

O primeiro bloco define a configuração da tela de apresentação:

gfxmenu (hd0,4)/message
: A `mensagem` da imagem de segundo plano localiza-se em `/dev/hda5`.

color white/blue black/light-gray
: Esquema de cor: branco (primeiro plano), azul (segundo plano), preto (seleção) e cinza-claro (segundo plano da seleção). O esquema de cores não tem efeito sobre

a tela de apresentação, apenas sobre o menu personalizável do GRUB que você pode acessar saindo da tela de apresentação com Esc.

default 0
Por padrão, a primeira entrada do menu, `title linux`, é a utilizada para inicializar.

timeout 8
Após oito segundos sem nenhuma entrada do usuário, o GRUB inicializa automaticamente a entrada default. Para desativar o boot automático, exclua a linha `timeout`. Se você definir `timeout 0`, o GRUB inicializa a entrada default imediatamente.

O segundo e maior bloco lista os vários sistemas operacionais inicializáveis. As seções para os sistemas operacionais individuais são introduzidas pelo `título`.

- A primeira entrada (`title linux`) é responsável por inicializar o SUSE Linux. O kernel (`vmlinuz`) localiza-se na primeira partição lógica (a partição de boot) do primeiro disco rígido. Os parâmetros do kernel, tais como a partição raiz e o modo VGA, são anexados aqui. A partição raiz é especificada de acordo com a convenção de nomenclatura do Linux (`/dev/hda7/`), pois essas informações são lidas pelo kernel e não têm nada a ver com o GRUB. O `initrd` também se localiza na primeira partição lógica do primeiro disco rígido.

- A segunda entrada é responsável por carregar o Windows. O Windows é inicializado a partir da primeira partição do primeiro disco rígido (`hd0,0`). O comando `chainloader +1` faz com que o GRUB leia e execute o primeiro setor da partição especificada.

- A próxima entrada permite o boot a partir do disco rígido sem modificar as configurações do BIOS.

- A opção de boot `failsafe` inicia o Linux com uma seleção de parâmetros do kernel que permite que o Linux seja inicializado nos sistemas problemáticos.

O arquivo de menu pode ser alterado sempre que for necessário. O GRUB utiliza, então, as configurações modificadas durante o próximo boot. Edite o arquivo permanentemente usando o YaST ou um editor da sua escolha. Como alternativa, faça as alterações temporárias de forma interativa usando a função de edição do GRUB. Consulte o item “Editando as entradas de menu durante o procedimento de boot” (p 461).

Editando as entradas de menu durante o procedimento de boot

No menu gráfico de boot do GRUB, selecione o sistema operacional a ser inicializado com as teclas de seta. Se selecionar um sistema Linux, você pode inserir parâmetros extras de boot no prompt de boot. Para editar diretamente as entradas individuais do menu, pressione Esc para sair da tela de apresentação e depois pressione E. As alterações feitas desta maneira só se aplicam ao procedimento atual de boot, não sendo adotadas permanentemente.

IMPORTANTE: Layout do teclado durante o procedimento de boot

O layout do teclado norte-americano é o único disponível na hora de inicializar.

Depois de ativar o modo de edição, use as teclas de seta para selecionar a entrada de menu cuja configuração deve ser editada. Para tornar a configuração editável, pressione E uma vez mais. Dessa maneira, edite as especificações incorretas das partições ou do caminho antes que tenham um efeito negativo sobre o processo de boot. Pressione Enter para sair do modo de edição e retornar ao menu. Depois pressione B para inicializar essa entrada. No texto de ajuda da parte inferior, são mostradas mais ações possíveis.

Para inserir permanentemente as opções alteradas de boot e passá-las para o kernel, abra o arquivo `menu.lst` como `raiz` do usuário e anexe os respectivos parâmetros do kernel à linha existente, separados por espaços:

```
title linux
   kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
   initrd (hd0,0)/initrd
```

O GRUB adota automaticamente os novos parâmetros na próxima vez em que o sistema é inicializado. Como alternativa, essa alteração também pode ser feita com o módulo do carregador de boot YaST. Anexe os novos parâmetros à linha existente, separados por espaços.

Usando curingas para selecionar o kernel de boot

Especialmente quando se desenvolvem ou se usam kernels personalizados, você deve mudar as entradas no `menu.lst` ou editar a linha de comando para refletir o kernel atual e os nomes de arquivos initrd. Para simplificar esse procedimento, use *curingas* para atualizar dinamicamente a lista do kernel do GRUB. Assim, todas as imagens do

kernel que correspondem a um padrão específico são automaticamente acrescentadas à lista de imagens inicializáveis. Observe que não há suporte a esse recurso.

Ative a opção do curinga inserindo uma entrada extra de menu no `menu.lst`. Para serem úteis, todas as imagens initrd e do kernel têm um nome-base comum e um identificador que corresponde ao kernel com o seu initrd associado. Considere a seguinte configuração:

```
initrd-default
initrd-test
vmlinuz-default
vmlinuz-test
```

Nesse caso, você pode acrescentar imagens de boot em uma configuração do GRUB. Para obter as entradas do menu `linux-default` e `linux-test`, seria necessária a seguinte entrada no `menu.lst`:

```
title linux-*
   wildcard (hd0,4)/vmlinuz-*
   kernel (hd0,4)/vmlinuz-* root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-*
```

Nesse exemplo, o GRUB pesquisa a partição (hd0,4) para ver se há entradas que correspondam ao curinga. Essas entradas são usadas para gerar novas entradas de menu do GRUB. No exemplo anterior, o GRUB comporta-se como se as seguintes entradas existissem no `menu.lst`:

```
title linux-default
   wildcard (hd0,4)/vmlinuz-default
   kernel (hd0,4)/vmlinuz-default root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-default
title linux-test
   wildcard (hd0,4)/vmlinuz-test
   kernel (hd0,4)/vmlinuz-test root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd-test
```

Com essa configuração, podem-se esperar problemas caso os nomes de arquivo não forem usados de forma consistente, ou se estiver faltando um dos arquivos expandidos, como uma imagem initrd.

29.3.2 O arquivo device.map

O arquivo `device.map` mapeia os nomes de dispositivos do GRUB para os nomes de dispositivos do Linux. Em um sistema misto que contém discos rígidos IDE e SCSI, o GRUB deve tentar determinar a seqüência de boot através de um procedimento

especial, pois o GRUB não tem acesso às informações do BIOS na seqüência de boot. O GRUB salva o resultado desta análise no arquivo `/boot/grub/device.map`. Para um sistema no qual a seqüência de boot no BIOS é configurada como IDE antes de SCSI, o arquivo `device.map` poderia aparecer da seguinte forma:

```
(fd0)   /dev/fd0
(hd0)   /dev/hda
(hd1)   /dev/sda
```

Como a ordem da IDE, da SCSI e de outros discos rígidos depende de vários fatores, e como o Linux não consegue identificar o mapeamento, a seqüência no arquivo `device.map` pode ser configurada manualmente. Se você encontrar problemas na hora do boot, verifique se a seqüência neste arquivo corresponde à seqüência no BIOS e use o shell do GRUB, descrito em Seção 29.3.4, “O shell do GRUB” (p 464), para modificá-la temporariamente, conforme se fizer necessário. Depois que o sistema Linux for inicializado, o arquivo `device.map` pode ser permanentemente editado com o módulo do carregador de boot YaST ou com um editor da sua preferência.

Depois de alterar manualmente o `device.map`, execute o seguinte comando para reinstalar o GRUB. Este comando faz com que o arquivo `device.map` seja recarregado e os comandos listados em `grub.conf` sejam executados:

```
grub --batch < /etc/grub.conf
```

29.3.3 O arquivo /etc/grub.conf

O terceiro arquivo importante de configuração do GRUB, depois do `menu.lst` e do `device.map`, é o `/etc/grub.conf`. Esse arquivo contém os parâmetros e as opções que o comando `grub` precisa para instalar corretamente o carregador de boot:

```
root (hd0,4)
   install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
   quit
```

Significado das entradas individuais:

root (hd0,4)
: Esse comando diz para o GRUB aplicar os seguintes comandos à primeira partição lógica do primeiro disco rígido (o local dos arquivos de boot).

install `parameter`

O comando `grub` deve ser executado com o parâmetro `install`. O `stage1` do carregador de boot deve ser instalado no MBR do primeiro disco rígido (`/grub/stage1 d (hd0)`). O `stage2` deve ser carregado no endereço de memória 0x8000 (`/grub/stage2 0x8000`). A última entrada (`(hd0,4)/grub/menu.lst`) mostra para o GRUB onde ele deve procurar o arquivo de menu.

29.3.4 O shell do GRUB

O GRUB existe em duas versões: como carregador de boot e como programa normal do Linux em `/usr/sbin/grub`. Esse programa é conhecido como *shell do GRUB*. A funcionalidade para instalar o GRUB como carregador de boot em um disco rígido ou em um disquete é integrada no GRUB na forma dos comandos `install` e `setup`. Isso está disponível no shell do GRUB quando o Linux é carregado.

No entanto, os comandos `setup` e `install` também estão disponíveis durante o procedimento de boot antes de o Linux ser iniciado. Isso facilita a reparação de um sistema com defeito que não pode mais ser inicializado, pois o arquivo de configuração defeituoso do carregador de boot pode ser evitado ao se inserir parâmetros manualmente. A inserção manual de parâmetros durante o procedimento de boot também é útil para testar novas configurações sem danificar o sistema nativo. Basta inserir o arquivo de configuração experimental com uma sintaxe semelhante àquela existente no `menu.lst`. Depois teste a funcionalidade dessa entrada sem alterar o arquivo de configuração atual. Por exemplo, para testar um novo kernel, insira o comando `kernel` e o caminho para o novo kernel. Se o procedimento de boot falhar, você poderá continuar a usar o arquivo `menu.lst` intacto na próxima vez em que inicializar o sistema. Da mesma forma, a interface da linha de comando também pode ser usada para inicializar um sistema apesar de um arquivo `menu.lst` defeituoso, inserindo-se os parâmetros corrigidos. No sistema em execução, os parâmetros corretos podem ser inseridos no `menu.lst` para tornar o sistema permanentemente inicializável.

O mapeamento dos dispositivos do GRUB com os nomes dos dispositivos do Linux só é relevante quando se executa o shell do GRUB como um programa Linux (inserindo-se `grub` como descrito em Seção 29.3.2, “O arquivo device.map” (p 462)). Para essa finalidade, o programa lê o arquivo `device.map`. Para obter mais informações, consulte o item Seção 29.3.2, “O arquivo device.map” (p 462).

29.3.5 Configurando uma senha de boot

Mesmo antes de o sistema operacional ser inicializado, o GRUB permite acesso aos sistema de arquivos. Os usuários que não têm permissões raiz podem acessar os arquivos no seu sistema Linux aos quais não têm acesso depois que o sistema é inicializado. Para bloquear esse tipo de acesso ou impedir que os usuários inicializem certos sistemas operacionais, defina uma senha de boot.

IMPORTANTE: Senha de boot e tela de apresentação

Se você usar uma senha de boot para o GRUB, a tela normal de apresentação não será exibida.

Como a `raiz` do usuário, proceda da seguinte forma para definir uma senha de boot:

1. No prompt raiz, insira `grub`.

2. Criptografe a senha no shell do GRUB:

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

3. Cole a string criptografada na seção global do arquivo `menu.lst`:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

   Agora os comandos do GRUB só podem ser executados no prompt raiz depois que se pressionar P e se inserir a senha. No entanto, os usuários ainda podem inicializar todos os sistemas operacionais a partir do menu de boot.

4. Para impedir que um ou vários sistemas operacionais sejam inicializados a partir do menu de boot, acrescente a entrada `lock` em cada seção no `menu.lst` que não deveria ser inicializada sem se inserir uma senha. Por exemplo:

```
title linux
kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
initrd (hd0,4)/initrd
lock
```

Depois de reiniciar o sistema e selecionar a entrada no Linux no menu de boot, é exibida a seguinte mensagem de erro:

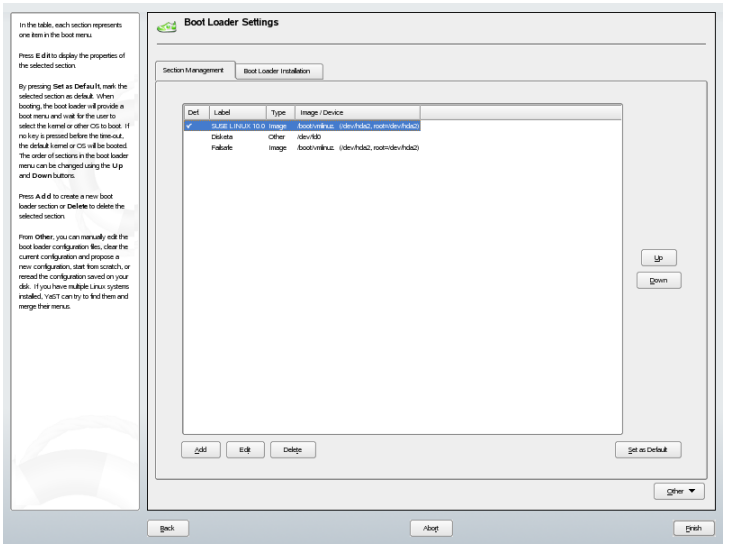
```
Erro 32: Precisa de autenticaç o
```

Pressione Enter para inserir o menu. Depois pressione P para obter o prompt da senha. Depois de inserir a senha e pressionar Enter, o sistema operacional selecionado (o Linux, neste caso) não deve inicializar.

29.4 Configurando o carregador de boot com o YaST

O modo mais fácil de configurar o carregador de boot em seu sistema SUSE Linux é utilizar o módulo do YaST. No Centro de Controle do YaST, selecione *Sistema → Configuração do Carregador de Boot*. A configuração atual do carregador de boot do sistema é exibida, possibilitando que você faça as mudanças desejadas. Consulte a Figura 29.1, “Configurando o carregador de boot com o YaST” (p 466).

Figura 29.1 *Configurando o carregador de boot com o YaST*



A janela principal consiste em duas guias:

Gerenciamento de Seções
Use esta guia para editar, mudar e apagar seções do carregador de boot referentes aos sistemas operacionais individuais. Para adicionar uma opção, clique em *Adicionar*. Para mudar o valor de uma opção existente, selecione-o com o mouse e clique em *Editar*. Se não quiser usar nenhuma opção existente, selecione-a e clique em *Apagar*. Se não estiver familiarizado com as opções do carregador de boot, leia primeiro a Seção 29.3, "Inicializando com o GRUB" (p 455).

Instalação do Carregador de Boot
Use esta guia para ver e mudar as configurações relacionadas a tipo, localização ou outras configurações do carregador de boot.

29.4.1 Tipo de Carregador de Boot

O tipo de carregador de boot é definido na guia *Instalação do Carregador de Boot*. O carregador de boot padrão no SUSE Linux é o GRUB. Para usar o LILO, proceda da seguinte maneira:

Procedimento 29.2 *Mudando o tipo de carregador de boot*

1. Abra a guia *Instalação do Carregador de Boot*.
2. No painel *Tipo*, clique no menu do *Carregador de Boot* e selecione *LILO*.
3. Selecione uma das seguintes ações do menu pop-up:

   Propor Nova Configuração
   O YaST propõe uma nova configuração.

   Converter Configuração Atual
   O YaST converte a configuração atual. Na conversão da configuração, algumas definições podem ser perdidas.

   Iniciar Nova Configuração do Início
   Use esta opção para gravar uma configuração personalizada. Esta ação não fica disponível durante a instalação do SUSE Linux.

   Ler Configuração Salva em Disco
   Use esta opção para carregar o seu próprio `/etc/lilo.conf`. Esta ação não fica disponível durante a instalação do SUSE Linux.

4 Clique em *OK* para gravar as mudanças.

5 Clique em *Concluir* na janela de diálogo principal para ativar as mudanças.

Após a conversão, a antiga configuração do GRUB é gravada no disco. Para utilizá-la, basta voltar o tipo de carregador de boot para GRUB e selecionar *Recuperar Configuração Salva Antes da Conversão* do menu pop-up. Esta ação fica disponível somente em um sistema instalado.

NOTA: Carregador de boot personalizado

Se quiser usar um carregador de boot que não seja o GRUB nem o LILO, clique na opção *Não Instalar Nenhum Carregador de Boot*. Leia a documentação do seu carregador de boot cuidadosamente antes de escolher esta opção.

29.4.2 Localização do carregador de boot

Pode ser necessário mudar a localização do carregador de boot. Este módulo do YaST o ajuda a fazer isso.

Procedimento 29.3 *Mudando a localização do carregador de boot*

1 Para mudar a localização do carregador de boot, clique na guia *Instalação do Carregador de Boot* e selecione as seguintes opções do menu *Localização do Carregador de Boot*:

MBR (Master Boot Record) de /dev/hdX
Registro mestre de inicialização de um disco. Esta opção é recomendada sempre que o SUSE determinar que o sistema pode ser inicializado desta maneira. O X identifica o disco rígido, isto é, a, b, c, d:

```
hda => ide0 master
     hdb => ide0 slave
     hdc => ide1 master
     hdd => ide1 slave
```

Setor de Boot da Partição de Boot /dev/hdXY
Setor de inicialização da partição `/boot`. Esta opção será padrão se você tiver vários sistemas operacionais instalados no disco rígido. O Y corresponde

à partição, isto é, 1, 2, 3, 4, 5 etc. A entrada, portanto, poderá ser semelhante a:

```
/dev/hda1
```

Setor de Boot da Partição Raiz /dev/hdXY
O setor de inicialização da partição / (raiz). Esta opção também será usada se você tiver vários sistemas operacionais instalados no disco rígido e quiser continuar usando o antigo gerenciador de inicialização.

Outros
Esta opção permite que você especifique a localização do carregador de boot.

2 Clique em *Concluir* para ativar as mudanças.

29.4.3 Sistema padrão

Para mudar o sistema padrão, proceda da seguinte maneira:

Procedimento 29.4 *Definindo o sistema padrão*

1 Abra a guia *Gerenciamento de Seções*.

2 Na lista, selecione o sistema desejado com o mouse ou clicando em *para cima* ou *para baixo*.

3 Clique em *Definir como Padrão*.

4 Clique em *Concluir* para ativar essas mudanças.

29.4.4 Tempo de espera do carregador de boot

O carregador de boot não inicializa o sistema padrão imediatamente. Durante este tempo de espera, é possível parar a reinicialização do sistema padrão e mudar o sistema a ser inicializado ou gravar alguns parâmetros do kernel. Para aumentar ou diminuir o tempo de espera do carregador de boot, proceda da seguinte maneira:

Procedimento 29.5 *Mudando o tempo de espera do carregador de boot*

1. Abra a guia *Instalação do Carregador de Boot*.
2. Clique em *Opções do Carregador de Boot*.
3. Marque a opção *Mostrar Menu de Boot*.
4. No *Menu de Boot*, mude o valor de *Tempo de Espera do Menu de Boot* digitando um novo valor, clicando na tecla de seta apropriada com o mouse ou utilizando as teclas de seta do teclado.
5. Clique em *OK*.
6. Clique em *Concluir* para ativar as mudanças.

Você pode decidir se o menu de inicialização deve ser exibido permanentemente sem contagem regressiva clicando na caixa *Continuar Boot após Tempo de Espera*.

29.4.5 Configurações de segurança

Utilizando este módulo do YaST, é possível definir uma senha para proteger o carregador de boot. Este procedimento aumenta o nível de segurança.

Procedimento 29.6 *Configurando a senha do carregador de boot*

1. Abra a guia *Instalação do Carregador de Boot*.
2. Clique em *Opções do Carregador de Boot*.
3. Em *Proteção por Senha*, marque a opção *Proteger Carregador de Boot com Senha* e defina a senha.
4. Clique em *OK*.
5. Clique em *Concluir* para ativar as mudanças.

29.4.6 Ordem do disco

Se o seu computador tiver mais de um disco rígido, é possível especificar a seqüência de inicialização dos discos, como definido no setup do BIOS da máquina (consulte a Seção 29.3.2, “O arquivo device.map” (p 462)). Para fazer isso, proceda da seguinte maneira:

Procedimento 29.7 *Configurando a ordem do disco*

1. Abra a guia *Instalação do Carregador de Boot*.
2. Clique em *Detalhes de Instalação do Carregador de Boot*.
3. Se mais de um disco for listado, selecione um disco e clique em *Para cima* ou *Para baixo* para reordenar os discos exibidos.
4. Clique em *OK* para gravar as mudanças.
5. Clique em *Concluir* para ativar as mudanças.

Utilizando este módulo, também é possível substituir o MBR por um código genérico (que inicializa a partição ativa). Clique em *Substituir MBR por Código Genérico* em *Atualização da Área do Sistema do Disco*. Também é possível clicar em *Ativar Partição do Carregador de Boot* no mesmo painel para ativar a partição que contém o carregador de boot. Clique em *Concluir* para ativar as mudanças.

29.5 Desinstalando a controladora de boot do Linux

O YaST pode ser usado para desinstalar o carregador de boot do Linux e recuperar o MBR para o estado que ele tinha antes da instalação do Linux. Durante a instalação, o YaST cria automaticamente uma cópia de backup do MBR original e o restaura sob solicitação, sobrescrevendo o GRUB.

Para desinstalar o GRUB, inicie o módulo do carregador de boot YaST (*Sistema* → *Configuração do Carregador de Boot*). Nessa primeira caixa de diálogo, selecione

Redefinir → Restaurar MBR do Disco Rígido e clique em *Concluir* para sair. No MBR, o GRUB é sobrescrito com os dados do MBR original.

29.6 Criando CDs de boot

Se a inicialização do sistema com um gerenciador de boot apresentar problemas ou se o gerenciador de boot não puder ser instalado no MBR do disco rígido ou do disquete, também será possível criar um CD inicializável com os arquivos de inicialização necessários para o Linux. É necessário haver um gravador de CD instalado no sistema.

A criação de um CR-ROM inicializável com GRUB requer simplesmente um formato especial de *stage2* chamado`stage2_eltorito` e, opcionalmente, um `menu.lst` personalizado. Os clássicos arquivos `stage1` e `stage2` não são necessários.

Crie um diretório para criação da imagem ISO, por exemplo, com `cd /tmp` e`mkdir iso`. Crie também um subdiretório para GRUM, com `mkdir -p iso/boot/grub`. Copie o arquivo `stage2_eltorito` no diretório `grub`:

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
```

Copie também o kernel (`/boot/vmlinuz`), o `initrd` (`/boot/initrd`) e o arquivo `/boot/message` em `iso/boot/`:

```
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
cp /boot/message iso/boot/
```

Para torná-los disponíveis para o GRUB, copie o arquivo `menu.lst` em `iso/boot/grub` e ajuste as entradas do caminho para que apontem para um dispositivo de CD-ROM. Faça isso substituindo o nome do dispositivo dos discos rígidos, listados no formato `(hd*)`, nos nomes de caminho, pelo nome de dispositivo da unidade do CD-ROM, que é `(cd)`:

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
    initrd (cd)/boot/initrd
```

Finalmente, crie a imagem ISO com o seguinte comando:

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Em seguida, grave o arquivo resultante `grub.iso` em um CD usando seu utilitário preferido.

29.7 A tela gráfica do SUSE

Desde o SUSE Linux 7.2, a tela gráfica do SUSE é exibida no primeiro console se a opção "vga=<value>" for usada como parâmetro de kernel. Se você fizer a instalação usando o YaST, essa opção é automaticamente ativada de acordo com a resolução e a placa de vídeo selecionadas. Há três maneiras de desativar a tela SUSE, se desejado:

Desabilitando a tela do SUSE quando necessário.
Insira o comando `echo 0 >/proc/splash` na linha de comando para desativar a tela gráfica. Para ativá-la novamente, insira `echo 1 >/proc/splash`.

Desabilitando a tela do SUSE por padrão.
Acrescente o parâmetro de kernel `splash=0` à configuração do seu carregador de boot. O Capítulo 29, *O Carregador de Boot* (p 453) fornece mais informações sobre isso. No entanto, se você preferir o modo de texto, que foi o padrão nas versões anteriores, configure `vga=normal`.

Desativando completamente a tela SUSE.
Compile um novo kernel e desative a opção *Usar a tela de apresentação em vez do logotipo de boot* no suporte a framebuffer.

DICA

A desabilitação do suporte a framebuffer no kernel também desabilita automaticamente a tela de apresentação. O SUSE não pode fornecer suporte ao seu sistema se você o executar com um kernel personalizado.

29.8 Solução de problemas

Essa seção lista alguns dos problemas freqüentemente encontrados na hora de inicializar com o GRUB e uma breve descrição das possíveis soluções. Alguns desses problemas

são analisados em artigos do Banco de Dados de Suporte, em http://portal.suse.de/sdb/en/index.html. Se o seu problema específico não estiver incluído nesta lista, use a caixa de diálogo de pesquisa do Banco de Dados de Suporte, no endereço https://portal.suse.com/PM/page/search.pm, para pesquisar palavras-chave como *GRUB*, *boot* e *carregador de boot*.

GRUB e XFS

O XFS não deixa espaço para o `stage1` no bloco de boot da partição. Portanto, não especifique uma partição XFS como local do carregador de boot. Esse problema pode ser resolvido com a criação de uma partição separada de boot que não é formatada com o XFS.

GRUB e JFS

Embora tecnicamente possível, a combinação do GRUB com o JFS é problemática. Nesse caso, crie uma partição de separada de boot (`/boot`) e formate-a com o Ext2. Instale o GRUB nessa partição.

O GRUB reporta um erro de geometria no GRUB

O GRUB verifica a geometria dos discos rígidos conectados quando o sistema é inicializado. Às vezes, a BIOS retorna informações inconsistentes e o GRUB cria um erro de geometria do GRUB. Se este for o caso, use o LILO ou atualize a BIOS. No Banco de Dados de Suporte, na palavra-chave LILO, há informações detalhadas sobre a instalação, configuração e manutenção do LILO.

O GRUB também retorna essa mensagem de erro se o Linux foi instalado em um disco rígido adicional que não está registrado no BIOS. O *stage1* do carregador de boot é encontrado e carregado corretamente, mas o *stage2* não é encontrado. Esse problema pode ser remediado registrando-se o novo disco rígido na BIOS.

O sistema contendo discos rígidos IDE e SCSI não inicializa

Durante a instalação, o YaST pode ter determinado incorretamente a seqüência de boot dos discos rígidos (e talvez você não a tenha corrigido). Por exemplo, o GRUB pode considerar `/dev/hda` como `hd0` e `/dev/sda` como `hd1`, embora a seqüência de boot no BIOS seja ao contrário (SCSI *antes* de IDE).

Nesse caso, corrija os discos rígidos durante o processo de boot com a ajuda da linha de comando do GRUB. Depois que o sistema for inicializado, edite o arquivo `device.map` para aplicar o novo mapeamento permanentemente. Depois verifique os nomes de dispositivo do GRUB nos arquivos `/boot/grub/menu.lst` e

`/boot/grub/device.map` e reinstale o carregador de boot com o seguinte comando:

```
grub --batch < /etc/grub.conf
```

Inicializando o Windows do segundo disco rígido

Alguns sistemas operacionais, como o Windows, podem ser inicializados apenas do primeiro disco rígido. Se um sistema operacional desse tipo for instalado em um disco rígido que não for o primeiro, você pode efetuar uma mudança lógica na respectiva entrada do menu.

```
...
title windows
map (hd0) (hd1)
map (hd1) (hd0)
chainloader(hd1,0)+1
...
```

Nesse exemplo, o Windows é iniciado a partir do segundo disco rígido. Para essa finalidade, a ordem lógica dos discos rígidos é alterada com `map`. Essa alteração não afeta a lógica dentro do arquivo de menu do GRUB. Portanto, o segundo disco rígido deve ser especificado para `chainloader`.

29.9 Mais informações

Em http://www.gnu.org/software/grub/, há informações abrangentes sobre o GRUB. Se texinfo for instalado na sua máquina, visite as páginas de informações do GRUB em um shell inserindo `info grub`. Você também pode pesquisar a palavra-chave “GRUB” no Banco de Dados de Suporte, em http://portal.suse.de/sdb/en/index.html, para obter informações sobre problemas específicos.

30 Recursos especiais do SUSE Linux

Este capítulo começa com informações sobre vários pacotes de software, os consoles virtuais e o layout de teclado. Abordamos componentes de software como `bash`, `cron` e `logrotate`, porque eles foram mudados ou aperfeiçoados durante os últimos ciclos de lançamento. Mesmo que eles sejam pequenos ou considerados de menor importância, talvez os usuários desejem mudar o seu comportamento padrão, porque esses componentes muitas vezes estão intimamente ligados ao sistema. O capítulo termina com uma seção sobre configurações específicas de país e idioma (I18N e L10N).

30.1 Informações sobre pacotes de software especiais

Os programas `bash`, `cron`, `logrotate`, `locate`, `ulimit` e `free`, e o arquivo `resolv.conf` são muito importantes para os administradores de sistema e para vários usuários. Páginas do manual e de informações são duas fontes úteis de informações sobre comandos, mas nem sempre ambas estão disponíveis. O GNU Emacs é um editor de texto popular e muito configurável.

30.1.1 O pacote bash e /etc/profile

Bash é o shell padrão no SUSE Linux. Quando usado com um shell de login, ele lê vários arquivos de inicialização. O Bash os processa na ordem que são exibidos na lista.

1. `/etc/profile`

2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Configurações personalizadas podem ser feitas em `~/.profile` ou em `~/.bashrc`. Para assegurar o processamento correto desses arquivos, é necessário copiar as configurações básicas de `/etc/skel/.profile` ou `/etc/skel/.bashrc` no diretório pessoal do usuário. É recomendável copiar as configurações de `/etc/skel` após uma atualização. Execute os seguintes comandos de shell para evitar a perda de ajustes pessoais:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Em seguida, copie os ajustes pessoais novamente dos arquivos `*.old`.

30.1.2 O pacote cron

Se você deseja executar comandos de maneira regular e automática em segundo plano, em momentos pré-definidos, o cron é a ferramenta tradicional a ser utilizada. O cron é regido por tabelas de tempo formatadas especialmente. Algumas delas são fornecidas com o sistema e os usuários podem gravar as suas próprias tabelas, se necessário.

As tabelas cron estão localizadas em `/var/spool/cron/tabs`. A `/etc/crontab` atua como uma tabela cron global do sistema. Digite o nome do usuário que deve executar o comando diretamente após da tabela de tempo. No Exemplo 30.1, “Entrada in /etc/crontab” (p 478), `root` é digitado. Tabelas específicas de pacote, localizadas em `/etc/cron.d`, possuem o mesmo formato. Consulte a página de manual `cron` (`man cron`).

Exemplo 30.1 *Entrada in /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Você não pode editar `/etc/crontab` chamando o comando `crontab -e`. Este arquivo deve ser carregado diretamente em um editor, modificado e, em seguida, gravado.

Alguns pacotes instalam scripts de shell nos diretórios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`, cujas instruções são controladas por `/usr/lib/cron/run-crons`. `/usr/lib/cron/run-crons` é executado a cada 15 minutos da tabela principal (`/etc/crontab`). Isso garante que os processos que tenham sido negligenciados possam ser executados no momento adequado.

Para executar os scripts de manutenção `por hora`, `di rio` ou outros scripts de manutenção periódica em horários personalizados, remova os arquivos de marcação de horário regularmente, utilizando as entradas `/etc/crontab` (consulte Exemplo 30.2, “/etc/crontab: Remoção de Arquivos de Marcação de Hora” (p 479), que remove a opção `por hora` antes de cada hora cheia, a opção `di rio` uma vez ao dia às 2h14, etc.).

Exemplo 30.2 *`/etc/crontab`: Remoção de Arquivos de Marcação de Hora*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Os trabalhos de manutenção diária de sistema foram distribuídos a vários scripts por motivos de clareza. Eles estão contidos no pacote `aaa_base`. `/etc/cron.daily` contém, por exemplo, os componentes `suse.de-backup-rpmdb`, `suse.de-clean-tmp` ou `suse.de-cron-local`.

30.1.3 Arquivos de registro: Pacote logrotate

Existem vários serviços de sistema (*daemons*) que, junto com o próprio kernel, gravam regularmente o status do sistema e eventos específicos em arquivos de registro. Desta maneira, o administrador pode verificar regularmente o status do sistema em um determinado momento, reconhecer erros ou funções defeituosas e solucioná-los com total precisão. Esses arquivos de registro são normalmente armazenados em `/var/log`, como especificado pelo FHS e crescem em uma base diária. O pacote `logrotate` ajuda a controlar o crescimento desses arquivos.

Configuração

Configure o logrotate com o arquivo `/etc/logrotate.conf`. Em particular, a especificação`include` configura principalmente os arquivos adicionais a serem lidos. O SUSE Linux assegura que os programas que produzem arquivos de registro instalam arquivos de configuração individual em `/etc/logrotate.d`. Por exemplo, tais programas acompanham os pacotes `apache2` (`/etc/logrotate.d/apache2`) e `syslogd` (`/etc/logrotate.d/syslog`).

Exemplo 30.3 *Exemplo para /etc/logrotate.conf*

```
# consulte "man lo rotate" para obter os detalhes
# rotacione os arquivos de registro semanalmente
semanalmente

# mantenha 4 semanas de backlogs
rotacione 4

# crie arquivos de registro novos (vazios) após rotacionar os antigos
criados

# ative esta opç o se deseja que os arquivos de registro sejam compactados
#compactar

# As informações de rotaç o de registro de drop de pacotes RPM neste diretório
 incluem
/etc/logrotate.d

# nenhum pacote possui lastlog ou wtmp - nós iremos rotacion -los aqui
#/var/log/wtmp {
#    mensal
#    criar 0664 root utmp
#    rotacionar 1
#}

# registros específicos de sistema também podem ser configurados aqui.
```

logrotate é controlado pelo cron e é chamado diariamente por `/etc/cron.daily/logrotate`.

IMPORTANTE

A opção `create` lê todas as configurações feitas pelo administrador em `/etc/permissions*`. Certifique-se de que não haja conflitos devido a modificações pessoais.

30.1.4 O comando locate

locate, um comando para localização rápida de arquivos, não está incluído no escopo padrão do software instalado. Se desejado, instale o pacote `find-locate`. O processo updatedb é iniciado automaticamente a cada noite ou aproximadamente 15 minutos após a inicialização do sistema.

30.1.5 O comando ulimit

Com o comando `ulimit` (*user limits*), é possível definir limites para o uso de recursos do sistema e fazer com que sejam exibidos. `ulimit` é particularmente útil para a limitação da memória disponível para aplicativos. Com ele, pode-se evitar que um aplicativo utilize muita memória, o que poderia travar o sistema.

O comando `ulimit` pode ser usado com várias opções. Para limitar o uso da memória, use as opções listadas na Tabela 30.1, “`ulimit`: Configuração de Recursos para o Usuário” (p 481).

Tabela 30.1 *ulimit: Configuração de Recursos para o Usuário*

`-m`	Tamanho máximo da memória física
`-v`	Tamanho máximo da memória virtual
`-s`	Tamanho máximo da pilha
`-c`	Tamanho máximo dos arquivos básicos
`-a`	Exibição de definição de limites

Configurações globais de sistema podem ser feitas em `/etc/profile`. Lá, habilite a criação de arquivos básicos, necessários para os programadores para *depuração*. Um usuário normal não pode aumentar os valores especificados em `/etc/profile` pelo administrador do sistema, mas pode fazer entradas especiais em `~/.bashrc`.

Exemplo 30.4 *ulimit: Configurações em ~/.bashrc*

```
# limite de memória física:
ulimit -m 98304

# limite de memória virtual:
ulimit -v 98304
```

As quantidades de memória devem ser especificadas em KB. Para obter informações mais detalhadas, consulte `man bash`.

IMPORTANTE

Nem todos os shells suportam as diretivas `ulimit`. O PAM (por exemplo, `pam_limits`) oferece possibilidades abrangentes de ajustes se você depende de configurações abrangentes para essas restrições.

30.1.6 O comando free

O comando `free` é um pouco confuso se a sua meta é determinar a quantidade de memória RAM usada no momento. Essas informações podem ser encontradas em `/proc/meminfo`. Atualmente, os usuários com acesso a um sistema operacional moderno, como o Linux, não precisam se preocupar muito com memória. O conceito de *RAM disponível* surgiu antes da época do gerenciamento unificado de memória. O slogan *memória livre é memória ruim* se aplica bem ao Linux. Como resultado, o Linux sempre se esforçou para equilibrar caches externos sem realmente permitir memória livre ou sem uso.

Basicamente, o kernel não tem conhecimento direto de nenhum aplicativo ou dados de usuário. Em vez disso, ele gerencia aplicativos e dados de usuário em um *cache de página*. Se a memória diminuir, partes dele são gravadas na partição de troca ou em arquivos, dos quais podem ser lidas inicialmente com a ajuda do comando `mmap` (consulte `man mmap`).

O kernel também contém outros caches, como o *cache slab*, onde os caches usados para acesso a rede são armazenados. Isso pode explicar as diferenças entre os contadores em `/proc/meminfo`. A maioria deles (mas não todos) pode ser acessada via `/proc/slabinfo`.

30.1.7 O arquivo /etc/resolv.conf

A resolução de nome de domínio é tratada pelo arquivo `/etc/resolv.conf`. Consulte o Capítulo 40, *Domain Name System (Sistema de Nomes de Domínio)* (p 633).

Este arquivo é atualizado pelo script `/sbin/modify_resolvconf` exclusivamente, e nenhum outro programa tem permissão para modificar diretamente o `/etc/resolv.conf`. Forçar esta regra é a única maneira de garantir que a configuração de rede do sistema e os arquivos relevantes sejam mantidos em um estado consistente.

30.1.8 Páginas de manual e de informações

Para alguns aplicativos GNU (como o tar), as páginas de manuais não são mais mantidas. Para esses comandos, use a opção `--help` para obter um rápido resumo das páginas de informações, que fornecem instruções mais detalhadas. O info é um sistema hipertexto do GNU. Leia uma introdução sobre este sistema digitando `info info`. As páginas de informações podem ser exibidas com Emacs ao se digitar `emacs -f info` ou diretamente em um console com `info`. Também é possível usar tkinfo, xinfo ou o sistema de ajuda do SUSE para exibir as páginas de informações.

30.1.9 Configurações para GNU Emacs

O GNU Emacs é um complexo ambiente de trabalho. As seções a seguir descrevem os arquivos de configuração processados quando o GNU Emacs é iniciado. Há mais informações em `http://www.gnu.org/software/emacs/`.

Na inicialização, o Emacs lê vários arquivos que contêm as configurações do usuário, administrador do sistema e distribuidor para personalização ou pré-configuração. O arquivo de inicialização `~/.emacs` é instalado nos diretórios pessoais dos usuários individuais a partir de `/etc/skel`. O `.emacs`, por sua vez, lê o arquivo `/etc/skel/.gnu-emacs`. Para personalizar o programa, copie o arquivo `.gnu-emacs` para o diretório pessoal (com `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) e faça as configurações desejadas nesse diretório.

O `.gnu-emacs` define o arquivo `~/.gnu-emacs-custom` como `arquivo personalizado`. Se os usuários fizerem as configurações com as opções

personalizar no Emacs, as configurações serão salvas no arquivo ~/.gnu-emacs-custom.

Com o SUSE Linux, o pacote do emacs instala o arquivo site-start.el no diretório /usr/share/emacs/site-lisp. O arquivo site-start.el é carregado antes do arquivo de inicialização ~/.emacs. Entre outras coisas, o arquivo site-start.el assegura que os arquivos de configuração especial distribuídos com os pacotes de expansão do Emacs, como o psgml, sejam carregados automaticamente. Os arquivos de configuração deste tipo estão localizados em /usr/share/emacs/site-lisp, também, e sempre começam com o nome suse-start-. O administrador do sistema local pode especificar configurações globais do sistema no arquivo default.el.

Mais informações sobre esses arquivos estão disponíveis no arquivo de informações do Emacs em *Init File*: info:/emacs/InitFile. Informações sobre como desabilitar o carregamento desses arquivos, se necessário, também são fornecidas neste local.

Os componentes do Emacs são divididos em vários pacotes:

- O pacote base emacs.
- emacs-x11 (normalmente instalado): o programa *com* suporte X11.
- emacs-nox: o programa *sem* suporte X11.
- emacs-info: documentação online em formato info.
- emacs-el: os arquivos de biblioteca não compilados em Emacs Lisp. Eles não são necessários em tempo de execução.
- Numerosos pacotes de expansão podem ser instalados, se houver necessidade: emacs-auctex (para LaTeX), psgml (para SGML e XML), gnuserv (para operação de cliente e servidor) e outros.

30.2 Consoles virtuais

O Linux é um sistema multiusuário e multitarefa. As vantagens desses recursos podem ser apreciadas mesmo em um sistema de PC independente. No modo de texto, existem

seis consoles virtuais disponíveis. Alterne entre eles utilizando a combinação de teclas Alt + F1 para Alt + F6. O sétimo console é reservado para X e o décimo console mostra as mensagens do kernel. Podem ser atribuídos mais ou menos consoles com a modificação do arquivo `/etc/inittab`.

Para alternar para um console de X sem fechá-lo, use a combinação de teclas Ctrl + Alt + F1 para Ctrl + Alt + F6. Para voltar para X, pressione Alt + F7.

30.3 Mapeamento de teclado

Para padronizar o mapeamento de teclado de programas, foram feitas mudanças nos seguintes arquivos:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Essas mudanças afetam apenas aplicativos que utilizam entradas `terminfo` ou cujos arquivos de configuração são mudados diretamente (`vi`, `less`, etc.). Os aplicativos que não acompanham o SUSE Linux devem ser adaptados a esses padrões.

Em X, a chave de composição (multikey) pode ser acessada utilizando Ctrl + Shift (direita). Consulte também a entrada correspondente em `/usr/X11R6/lib/X11/Xmodmap`.

Outras configurações são possíveis utilizando a Extensão de Teclado X (XKB). Esta extensão também é usada pelos ambientes de área de trabalho do GNOME (gswitchit) e KDE (kxkb).

DICA: Mais informações

Informações sobre o XKB estão disponíveis em `/etc/X11/xkb/README` e nos documentos ali relacionados.

Informações detalhadas sobre a entrada dos idiomas chinês, japonês e coreano (CJK) estão disponíveis na página de Mike Fabian em: http://www.suse.de/~mfabian/suse-cjk/input.html.

30.4 Configurações de idioma e específicas de país

O SUSE Linux é amplamente internacionalizado e pode ser modificado para satisfazer as necessidades locais de maneira flexível. Em outras palavras, a internacionalização (*I18N*) permite localizações específicas (*L10N*). As abreviações I18N e L10N são derivadas das primeiras e últimas letras das palavras e, no meio, está o número de letras omitidas.

As configurações são feitas com variáveis `LC_` definidas no arquivo `/etc/sysconfig/language`. Estas referem-se não somente ao *suporte ao idioma nativo*, mas também às categorias*Mensagens* (Idioma), *Conjunto de Caracteres*, *Ordem de Classificação*, *Hora e Data*, *Números* e *Moeda*. Cada uma dessas categorias pode ser definida diretamente com sua própria variável ou indiretamente com uma variável master no arquivo `language` (consulte a página de manual `local`).

RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME, RC_LC_NUMERIC, RC_LC_MONETARY
: Essas variáveis são passadas para o shell sem o prefixo `RC_` e representa as categorias listadas. Os perfis shell de referência estão listados abaixo. A configuração atual pode ser exibida com o comando `locale`.

RC_LC_ALL
: Esta variável, se definida, sobregrava os valores das variáveis já mencionadas.

RC_LANG
: Se nenhuma das variáveis anteriores for definida, este é o fallback. Por padrão, o SUSE Linux apenas define `RC_LANG`. Isto facilita o processo para que os usuários informem seus próprios valores.

ROOT_USES_LANG
: Uma variável `yes` ou `no`. Se for definida como `no`, `root` sempre funcionará no ambiente POSIX.

As outras variáveis podem ser definidas via editor sysconfig do YaST (consulte Seção 28.3.1, “Mudando a configuração do sistema usando o Editor sysconfig do YaST” (p 450)). O valor de tal variável contém o código do idioma, código do país, codificação e modificador. Os componentes individuais são conectados por caracteres especiais:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

30.4.1 Alguns exemplos

Você deve sempre definir os códigos do idioma e do país juntos. As configurações do idioma seguem o padrão ISO 639 disponível em `http://www.evertype.com/standards/iso639/iso639-en.html` e `http://www.loc.gov/standards/iso639-2/`. Os códigos de país estão listados na variável ISO 3166 disponível em `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`.

Só faz sentido definir valores para os quais os arquivos de descrição utilizáveis podem ser encontrados em `/usr/lib/locale`. Arquivos de descrição adicionais podem ser criados de arquivos em `/usr/share/i18n` utilizando o comando `localedef`. Os arquivos de descrição fazem parte do pacote `glibc-i18ndata`. Um arquivo de descrição para `en_US.UTF-8` (para inglês e Estados Unidos) pode ser criado com:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

`LANG=en_US.UTF-8`
: Esta é a configuração padrão se Inglês americano for selecionado durante a instalação. Se você selecionou outro idioma, aquele idioma será habilitado, mas ainda com o UTF-8 como a codificação de caractere.

`LANG=en_US.ISO-8859-1`
: Este define o idioma para inglês, país para Estados Unidos e a definição de caractere para `ISO-8859-1`. Esta definição de caractere não suporta o sinal de Euro, mas às vezes pode ser útil para programas que não foram atualizados para suportar `UTF-8`. A string que define o conjunto de caracteres (`ISO-8859-1` neste caso) é então avaliada por programas como o Emacs.

`LANG=en_IE@euro`
: O exemplo acima inclui explicitamente o sinal de Euro em uma configuração de idioma. Falando estritamente, esta configuração é atualmente obsoleta, porque o

UTF-8 também cobre o símbolo de Euro. Ela é útil apenas se um aplicativo não suportar o UTF-8, mas o ISO-8859-15.

O SuSEconfig lê as variáveis em `/etc/sysconfig/language` e grava as mudanças necessárias em `/etc/SuSEconfig/profile` e `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` é lido ou *originado* por `/etc/profile`. `/etc/SuSEconfig/csh.cshrc` é originado por `/etc/csh.cshrc`. Isso torna as configurações disponíveis em todo o sistema.

Os usuários anular os padrões do sistema editando o seu `~/.bashrc` de acordo. Por exemplo, se você não quiser usar o `en_US` global de sistema para mensagens de programa, inclua `LC_MESSAGES=es_ES`, então as mensagens serão exibidas em espanhol.

30.4.2 Configurações de suporte de idioma

Arquivos na categoria *Mensagens* são, como regra, armazenados somente no diretório do idioma correspondente (como `en`) para ter um fallback. Se você definir `LANG` para `en_US` e o arquivo de mensagem em `/usr/share/locale/en_US/LC_MESSAGES` não existir, ele voltará para `/usr/share/locale/en/LC_MESSAGES`.

Uma cadeia de fallback também pode ser definida, por exemplo, para bretão para francês ou galego para espanhol para português:

```
LANGUAGE="br_FR:fr_FR"

LANGUAGE="gl_ES:es_ES:pt_PT"
```

Se desejado, use as variantes noruegas Nynorsk e Bokmål (com fallback adicional para `no`):

```
LANG="nn_NO"

LANGUAGE="nn_NO:nb_NO:no"
```

ou

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Observe que em norueguês, `LC_TIME` também é tratado de maneira diferente.

Um problema que pode surgir é um separador usado para delimitar grupos de dígitos não ser reconhecido corretamente. Isso acontece se `LANG` for definido para um código de idioma com somente duas letras, como `de`, mas o arquivo de definição que o glibc utiliza está localizado em `/usr/share/lib/de_DE/LC_NUMERIC`. Por isso, `LC_NUMERIC` deve ser definido para `de_DE` para tornar a definição de separador visível para o sistema.

30.4.3 Mais informações

- *The GNU C Library Reference Manual*, Capítulo “Locales and Internationalization”. Ele está incluído em `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, atualmente em `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.
- *Unicode-Howto*, de Bruno Haible: `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

31 Operação da impressora

CUPS é o sistema de impressão padrão do SUSE Linux. O CUPS é altamente orientado ao usuário. Em muitos casos, é compatível com LPRng ou pode ser adaptado com relativamente pouco esforço. O LPRng é incluído no SUSE Linux apenas por motivos de compatibilidade.

As impressoras podem ser distinguidas pela interface, como USB ou rede, e pela linguagem de impressão. Ao comprar uma impressora, verifique se a interface do equipamento é suportada pelo hardware e se a linguagem da impressora é adequada. As impressoras podem ser categorizadas com base em três classes de linguagem:

Impressoras PostScript
PostScript é a linguagem de impressora na qual a maior parte dos trabalhos de impressão Linux e Unix são gerados e processados pelo sistema de impressão interno. Essa linguagem já existe há bastante tempo e é muito eficiente. Se documentos PostScript puderem ser diretamente processados pela impressora e não precisarem ser convertidos em estágios adicionais do sistema de impressão, o número de origens de erro potenciais será reduzido. Como as impressoras PostScript estão sujeitas a custos de licenciamento substanciais, elas geralmente custam mais que as impressoras sem interpretador PostScript.

Impressora padrão (linguagens como PCL e ESC/P)
Embora essas linguagens de impressora tenham surgido há bastante tempo, ainda são usadas e sofrem constantes desenvolvimentos para se adaptarem aos novos recursos de impressoras. No caso de linguagens conhecidas, o sistema pode converter tarefas de impressão PostScript na respectiva linguagem de impressão com a ajuda do Ghostscript. Esse estágio de processamento é chamado de interpretação. As linguagens mais conhecidas são a PCL, mais usada pelas impressoras HP e seus

clones, e a ESC/P, utilizada nas impressoras Epson. Geralmente, essas linguagens são suportadas no Linux e produzem um resultado de impressão satisfatório. Pode ocorrer de o Linux não conseguir lidar com algumas funções de impressoras muito novas e sofisticadas, já que os desenvolvedores do código-fonte aberto ainda estarão trabalhando nesses recursos. Além da HP, que desenvolve os drivers `hpijs`, nenhum outro fabricante cria ou disponibiliza drivers Linux aos distribuidores como licença de código-fonte aberto. A maior parte dessas impressoras está na faixa de preços intermediária.

Impressoras proprietárias (geralmente, impressoras GDI)
Em geral, apenas um ou vários drivers Windows estão disponíveis para impressoras proprietárias. Essas impressoras não aceitam nenhuma das linguagens de impressão comuns, e as que usam estão sujeitas a alteração quando uma nova edição de um modelo é lançada. Consulte a Seção 31.7.1, “Impressoras sem suporte de linguagem de impressora padrão” (p 508) para obter mais informações.

Antes de comprar uma nova impressora, consulte as seguintes fontes para verificar a abrangência do suporte ao equipamento pretendido:

- `http://cdb.suse.de/` — banco de dados de impressoras do SUSE Linux
- `http://www.linuxprinting.org/` — banco de dados de impressoras do site LinuxPrinting.org
- `http://www.cs.wisc.edu/~ghost/` — site do Ghostscript na Web
- `/usr/share/doc/packages/ghostscript/catalog.devices` — lista de drivers incluídos

Os bancos de dados online sempre mostram o status de suporte Linux mais recente. No entanto, a distribuição do Linux só pode integrar os drivers disponíveis no momento da produção. Da mesma forma, uma impressora atualmente classificada como “perfeitamente suportada” poderá não apresentar esse status quando a próxima versão do SUSE Linux for lançada. Assim, os bancos de dados não indicarão necessariamente o status correto, mas apenas uma informação aproximada.

31.1 Fluxo de trabalho do sistema de impressão

O usuário cria uma tarefa de impressão. Essa tarefa consiste nos dados a serem impressos, além de informações para o spooler, como nome da impressora ou nome da fila de impressão e, opcionalmente, dados para o filtro, como opções específicas da impressora.

Existe uma fila de impressão dedicada para cada impressora. O spooler mantém a tarefa de impressão em fila até que a impressora desejada esteja pronta para receber dados. Uma vez pronta, o spooler envia os dados pelo filtro, tendo a impressora como back end.

O filtro converte os dados que o usuário deseja imprimir (ASCII, PostScript, PDF, JPEG etc.) em dados específicos de impressora (PostScript, PCL, ESC/P etc.). Os recursos da impressora são descritos nos arquivos PPD. O arquivo PPD contém opções da impressora com os parâmetros necessários para habilitá-los. O sistema de filtros verifica se as opções selecionadas pelo usuário foram habilitadas.

Se você usa uma impressora PostScript, o sistema de filtros converte os dados em PostScript específico da impressora. Isso não exige um driver de impressora. Se você usa uma impressora não-PostScript, o sistema de filtros converte os dados em dados específicos da impressora usando o Ghostscript. Isso exige um driver Ghostscript adequado à sua impressora. O back end recebe do filtro os dados específicos da impressora e os repassa a ela.

31.2 Métodos e protocolos de conexão de impressoras

Existem várias possibilidades para conectar uma impressora ao sistema. A configuração do sistema de impressão CUPS não faz distinção entre uma impressora local e uma impressora conectada ao sistema pela rede. No Linux, impressoras locais devem ser conectadas conforme descrito no manual do respectivo fabricante. O CUPS suporta conexões seriais, USB, paralelas e SCSI. Para obter mais informações sobre a conexão de impressoras, leia o artigo *CUPS in a Nutshell* (Aprendendo mais um pouco sobre

CUPs) no Banco de Dados de Suporte, em http://portal.suse.com. Para encontrar o artigo, digite *cups* na caixa de diálogo de pesquisa.

ATENÇÃO: Conexão do cabo à máquina

Ao conectar a impressora à máquina, não esqueça de que apenas dispositivos USB podem ser conectados ou desconectados durante a operação. Desligue o sistema antes de modificar outros tipos de conexão.

31.3 Instalação do software

PPD (descrição de impressora PostScript) é a linguagem de computador que descreve as propriedades, como resolução, e as opções, como disponibilidade de uma unidade duplex. Essas descrições são necessárias para o uso de várias opções de impressora no CUPS. Sem um arquivo PPD, os dados de impressão seriam encaminhados à impressora em estado "bruto", o que normalmente não é desejado. Durante a instalação do SUSE Linux, vários arquivos PPD são pré-instalados, habilitando o uso de até mesmo impressoras sem suporte a PostScript.

Para configurar uma impressora PostScript, a melhor opção é obter um arquivo PPD adequado. Há vários arquivos PPD disponíveis no pacote de `PPDs do fabricante`, que são automaticamente instalados no escopo da instalação padrão. Consulte a Seção 31.6.3, "Arquivos PPD em pacotes diferentes" (p 505) e a Seção 31.7.2, "Nenhum arquivo PPD adequado disponível para impressora PostScript" (p 508).

Novos arquivos PPD podem ser armazenados no diretório `/usr/share/cups/model/` ou adicionados ao sistema de impressão por meio do YaST (consulte a "Configuração manual" (p 496)). Posteriormente, é possível selecionar o arquivo PPD durante a instalação.

Tenha cuidado se o fabricante pedir que você instale pacotes de software inteiros para modificar arquivos de configuração. Em primeiro lugar, esse tipo de instalação pode resultar na perda do suporte oferecido pelo SUSE Linux. Em segundo lugar, os comandos de impressão poderão funcionar de forma diferente, e talvez o sistema não consiga abordar dispositivos de outros fabricantes. Por isso, não recomendamos instalar o software do fabricante.

31.4 Configuração da impressora

Após conectar a impressora ao computador e instalar o software, instale a impressora no sistema. Faça isso usando as ferramentas que acompanham o SUSE Linux. Como o SUSE Linux enfatiza a segurança, ferramentas de terceiros não funcionarão bem com as restrições de segurança e causarão mais problemas que benefícios. Consulte a Seção 31.6.1, “Servidor e firewall do CUPS” (p 502) e a Seção 31.6.2, “Mudanças no serviço de impressão do CUPS” (p 503) para obter mais informações sobre como solucionar problemas.

31.4.1 Impressoras locais

Se for detectada uma impressora local não configurada quando você efetuar login, o YaST será iniciado para configurá-la. Serão usadas as mesmas caixas de diálogo mostradas abaixo para a descrição da configuração.

Para configurar a impressora, selecione *Hardware* → *Impressora* no centro de controle do YaST. Isso abrirá a janela de configuração principal da impressora, onde os dispositivos detectados são listados na parte superior. A parte inferior relaciona as listas configuradas até então. Se sua impressora não foi detectada, configure-a manualmente.

IMPORTANTE

Se a entrada *Impressora* não estiver disponível no centro de controle do YaST, provavelmente o pacote `yast2-printer` não está instalado. Para solucionar esse problema, instale o pacote `yast2-printer` e reinicie o YaST.

Configuração automática

O YaST poderá configurar a impressora automaticamente se for possível configurar automaticamente a porta paralela ou USB e se a impressora conectada puder ser detectada. O banco de dados da impressora também deve conter a string do ID da impressora que o YaST recupera durante a detecção automática do hardware. Se o ID do hardware for diferente do da designação do modelo, selecione o modelo manualmente.

Para assegurar que tudo funcione adequadamente, cada configuração deve ser verificada com a função de teste de impressão do YaST. A página de teste também fornece informações importantes sobre a configuração testada.

Configuração manual

Se os requisitos da configuração automática não forem atendidos, ou se você quiser fazer uma configuração personalizada, configure a impressora manualmente. Dependendo do sucesso da detecção automática e da quantidade de informações sobre o modelo de impressora encontradas no banco de dados, o YaST poderá determinar as configurações corretas automaticamente ou, pelo menos, fazer uma pré-seleção razoável.

Os seguintes parâmetros devem ser configurados:

Conexão de Hardware (Porta)
A configuração da conexão de hardware dependerá da habilidade do YaST em encontrar a impressora durante a detecção automática de hardware. Se o YaST conseguir detectar o modelo de impressora automaticamente, poderemos deduzir que a conexão da impressora está funcionando no nível de hardware, não sendo necessário modificar qualquer configuração a esse respeito. Se o YaST não conseguir detectar automaticamente o modelo de impressora, poderá haver algum problema na conexão no nível do hardware. Nesse caso, será necessária alguma intervenção manual para configurar a conexão.

Na caixa de diálogo *Configuração da Impressora*, pressione *Configurar* para iniciar o fluxo de trabalho de configuração manual. Selecione o *Tipo de Impressora* (por exemplo, `Impressora USB`) e, clicando em *Próximo*, digite a *Conexão de Impressora* e selecione o dispositivo.

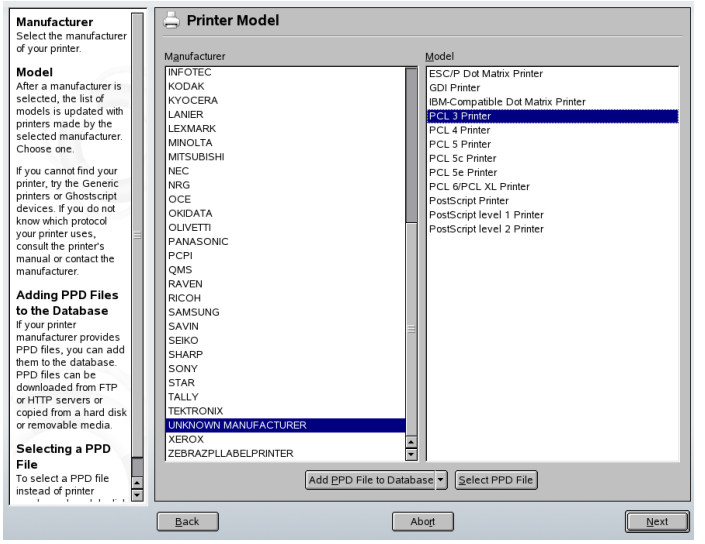
Nome da Fila
O nome da fila é usado quando emitimos comandos de impressão. O nome deve ser relativamente curto e composto apenas por letras minúsculas e números. Digite o *Nome para impressão* na próxima caixa de diálogo (*Nome da fila*).

Modelo de Impressora e Arquivo PPD
Todos os parâmetros específicos da impressora, como o driver Ghostscript a ser usado e os parâmetros do filtro de impressão, são armazenados em um arquivo PPD (PostDescription Printer Description). Consulte Seção 31.3, “Instalação do software” (p 494) para obter mais informações sobre arquivos PPD.

Para muitos modelos de impressora, haverá vários arquivos PPD disponíveis se, por exemplo, vários drivers Ghostscript funcionarem com o modelo em questão. Quando você selecionar um fabricante e um modelo na próxima caixa de diálogo (*Modelo de impressora*), o YaST selecionará o arquivo PPD que corresponde à impressora. Se houver vários arquivos PPD disponíveis para o modelo, o YaST assumirá um deles como padrão (normalmente aquele marcado como `recomendado`). É possível modificar o arquivo PPD escolhido na próxima caixa de diálogo usando *Editar*.

Para modelos não-PostScript, todos os dados específicos da impressora são produzidos pelo driver Ghostscript. Por esse motivo, a configuração do driver é o fator mais importante a determinar a qualidade da impressão. A impressão é afetada pelo tipo de driver Ghostscript (arquivo PPD) selecionado e pelas opções especificadas para ele. Se necessário, mude as opções adicionais (conforme disponibilizadas pelo arquivo PPD) depois de selecionar *Editar*.

Figura 31.1 *Seleção do modelo de impressora*



Sempre verifique se suas configurações estão funcionando como esperado. Para isso, imprima a página de teste. Se a impressão sair com erros (por exemplo, com várias páginas praticamente vazias), pare a impressão removendo todo o papel e, em seguida, interrompendo o teste no YaST.

Se o banco de dados da impressora não incluir uma entrada para o modelo, será possível adicionar um novo arquivo PPD selecionando *Adicionando Arquivo PPD ao Banco de Dados* ou usando um grupo de arquivos PPD genéricos para forçar a impressora a usar uma das linguagens de impressão padrão. Para isso, selecione *FABRICANTE DESCONHECIDO* como fabricante da impressora.

Configurações Avançadas
Normalmente, não é necessário alterar essas configurações.

31.4.2 Impressoras de rede

Uma impressora de rede pode suportar vários protocolos, alguns deles simultaneamente. Embora a maioria dos protocolos suportados sejam padronizados, alguns fabricantes expandem (modificam) o padrão porque eles testam sistemas que não implementaram o padrão corretamente ou porque querem fornecer certas funções que não estão disponíveis no padrão. Os fabricantes fornecem drivers apenas para alguns sistemas operacionais, eliminando dificuldades relativas a eles. Infelizmente, raros são os drivers para Linux. Na situação atual, não é possível agir como se todos os protocolos funcionassem perfeitamente no Linux. Portanto, talvez seja necessário testar várias opções para obter uma configuração funcional.

O CUPS suporta os protocolos `soquete`, `LPD`, `IPP` e `smb`. Veja abaixo alguns detalhes sobre esses protocolos:

soquete
Soquete se refere a uma conexão na qual os dados são enviados a um soquete de Internet sem precedência de handshake de dados. Alguns dos números de portas de soquete normalmente usados são `9100` ou `35`. Um exemplo de URI de dispositivo é `socket://host-printer:9100/`.

LPD (daemon de impressora de linha)
O protocolo LPD comprovado é descrito em RFC 1179. Nesse protocolo, alguns dados relativos à tarefa, como ID da fila de impressão, são enviados antes dos dados de impressão propriamente ditos. Portanto, deve ser especificada uma fila de impressão durante a configuração do protocolo LPD para a transmissão de dados. As implementações de fabricantes de impressoras diferentes são flexíveis o suficiente para aceitar qualquer nome como fila de impressão. Se necessário, o manual da impressora indicará o nome a ser usado. LPT, LPT1, LP1 ou semelhantes são os nomes normalmente usados. Também é possível configurar uma fila LPD em um

host Linux ou Unix diferente no sistema CUPS. O número de porta para o serviço LPD é `515`. Um exemplo de URI de dispositivo é `lpd://host-printer/LPT1`.

IPP (protocolo de impressão de Internet)
O IPP é um protocolo relativamente novo (1999) baseado no protocolo HTTP. Com o IPP, mais dados referentes à tarefa são transmitidos. O CUPS usa o IPP em transmissões internas de dados. É o protocolo escolhido para a fila de encaminhamento entre dois servidores CUPS. É necessário indicar o nome da fila de impressão para que o IPP seja configurado corretamente. A porta padrão do IPP é `631`. Exemplos de URIs de dispositivo são `ipp://host-printer/ps` e `ipp://host-cupsserver/printers/ps`.

SMB (compartilhamento Windows)
O CUPS também suporta a impressão em impressoras conectadas a compartilhamentos Windows. O protocolo usado para essa finalidade é o SMB. O SMB usa os números de porta `137`, `138` e `139`. Exemplos de URIs de dispositivos são `smb://user:password@workgroup/server/printer`, `smb://user:password@host/printer` e `smb://server/printer`.

O protocolo suportado pela impressora deve ser determinado antes da configuração. Se o fabricante não fornecer as informações necessárias, o comando `nmap`, que vem com o pacote `nmap`, poderá ser usado para descobrir o protocolo. `nmap` verificar as portas abertas do host. Por exemplo:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

Configuração do CUPS na rede com YaST

As impressoras de rede devem ser configuradas com o YaST. O YaST facilita a configuração e é mais bem equipado para lidar com restrições de segurança no CUPS (consulte a Seção 31.6.2, “Mudanças no serviço de impressão do CUPS” (p 503)). Para obter orientações sobre a instalação do CUPS na rede, leia o artigo *CUPS in a Nutshell* no Banco de Dados de Suporte, em `http://portal.suse.com`.

Selecione Outro (não detectado) e clique em *Configurar*. Se não houver orientação contrária do administrador de rede, tente a opção *Imprimir Diretamente em Impressora de Rede* e prossiga de acordo com os requisitos locais.

Configuração com ferramentas da linha de comando

O CUPS também pode ser configurado com ferramentas de linha de comando como `lpadmin` e `lpoptions`. Você precisará de um URI de dispositivo consistente em um back end, como usb, e parâmetros como `/dev/usb/lp0`. Por exemplo, o URI completo poderia ser `parallel:/dev/lp0` (impressora conectada à primeira porta paralela) ou `usb:/dev/usb/lp0` (primeira impressora conectada à porta USB).

Com `lpadmin`, o administrador do servidor CUPS pode adicionar, remover ou gerenciar filas de classe e de impressão. Para adicionar uma fila de impressão, use a seguinte sintaxe:

```
lpadmin -p queue -v device-URI \
-P PPD-file -E
```

O dispositivo (`-v`) estará disponível como *`fila`* (`-p`), usando o arquivo PPD especificado (`-P`). Isso significa que você deve conhecer o arquivo PPD e o nome do dispositivo se quiser configurar a impressora manualmente.

Não use `-E` como primeira opção. Em todos os comandos CUPS, `-E` como primeiro argumento define o uso de uma conexão criptografada. Para habilitar a impressora, `-E` deve ser usado como mostrado no seguinte exemplo:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

O seguinte exemplo configura uma impressora de rede:

```
lpadmin -p ps -v socket://192.168.1.0:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Para obter mais opções de `lpadmin`, consulte a página de manual `lpadmin(1)`.

Durante a instalação do sistema, algumas opções são definidas como padrão. Essas opções podem ser modificadas para cada tarefa de impressão (dependendo da ferramenta de impressão utilizada). Também é possível modificar essas opções padrão com o YaST. Usando ferramentas de linha de comando, defina opções padrão da seguinte forma:

1. Primeiro, liste todas as opções:

   ```
   lpoptions -p queue -l
   ```

   Exemplo:

   ```
   Resoluç o/Resoluç o de Saída: 150dpi *300dpi 600dpi
   ```

A opção padrão ativada fica evidente com o asterisco precedente (*).

2 Mude a opção com `lpadmin`:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Verifique a nova configuração:

```
lpoptions -p queue -l

Resoluç o/Resoluç o de Saída: 150dpi 300dpi *600dpi
```

Quando um usuário comum executa `lpoptions`, as configurações são gravadas em `~/.lpoptions`. As configurações de `root` são gravadas em `/etc/cups/lpoptions`.

31.5 Configuração de aplicativos

Os aplicativos, assim como as ferramentas da linha de comando, dependem das filas de impressora existentes. Geralmente, não é necessário reconfigurar a impressora de um aplicativo específico porque provavelmente você conseguirá imprimir usando as filas disponíveis.

Para imprimir da linha de comando, digite `lp-d` *`nome da fila nome do arquivo`*, substituindo os nomes correspondentes do *`nome da fila`* e *`nome do arquivo`*.

Alguns aplicativos dependem do comando `lp` para imprimir. Nesse caso, digite o comando correto na caixa de diálogo do aplicativo, geralmente sem especificar *`nome do arquivo`*, por exemplo `lp -d`*`nome da fila`*. Para que isso funcione com programas KDE, habilite *Impressão através de programa externo*. Caso contrário, você não poderá digitar o comando de impressão.

Ferramentas como o xpp e o programa kprinter do KDE oferecem uma interface gráfica que permite escolher filas e definir opções padrão do CUPS e específicas da impressora disponibilizadas por meio do arquivo PPD. Você pode usar o kprinter como interface de impressão padrão de aplicativos não KDE especificando `kprinter` ou `kprinter--stdin` como comando de impressão nas caixas de diálogo desses aplicativos. O comportamento do aplicativo determinará o comando a ser escolhido. Se configurado corretamente, o aplicativo deverá chamar a caixa de diálogo kprinter

sempre que uma tarefa de impressão for emitida. Por isso, você pode usar a caixa de diálogo para selecionar uma fila e definir outras opções de impressão. Isso requer que a configuração de impressão do próprio aplicativo não conflite com a do kprinter, e que as opções de impressão somente sejam modificadas por meio de kprinter depois que este seja habilitado.

31.6 Recursos especiais do SUSE Linux

Vários recursos do CUPS foram adaptados para o SUSE Linux. Algumas das mudanças mais importantes são abordadas aqui.

31.6.1 Servidor e firewall do CUPS

Existem várias maneiras de configurar o CUPS como cliente de um servidor de rede.

1. Para cada fila do servidor de rede, você pode configurar uma fila local por meio da qual encaminhará todas as tarefas ao servidor de rede correspondente. Geralmente, essa abordagem não é recomendada porque todas as máquinas clientes devem ser reconfiguradas sempre que a configuração do servidor de rede sofrer alguma mudança.

2. As tarefas de impressão também podem ser encaminhadas diretamente a um servidor de rede. Para esse tipo de configuração, não execute um daemon CUPS local. A chamada de `lp` ou da biblioteca correspondente de outros programas pode enviar tarefas diretamente ao servidor de rede. No entanto, essa configuração não funcionará se você também quiser imprimir em uma impressora local.

3. O daemon CUPS pode ouvir pacotes de transmissão IPP que outros servidores de rede enviam para anunciar as filas disponíveis. Para usar esse método, a porta 631/UDP deve estar aberta para pacotes de entrada.

   Essa é a melhor configuração do CUPS para impressão em servidores CUPS remotos. No entanto, há o risco de que um invasor envie transmissões IPP com filas e o daemon local acesse uma fila falsa. Se ele exibir a fila com o mesmo nome de outra fila no servidor local, o proprietário da tarefa poderá acreditar

que a tarefa foi enviada a um servidor local, enquanto, na verdade, ela foi enviada ao servidor do invasor.

O YaST pode localizar os servidores CUPS verificando todos os hosts de rede para ver se eles oferecem esse serviço e ouvindo transmissões IPP. O segundo método é usado durante a instalação do sistema para localizar servidores CUPS para a proposta. Ele exige que a porta 631/UDP esteja aberta para pacotes de entrada. Abrir uma porta para configurar acesso a filas remotas por meio do segundo método pode constituir um risco de segurança porque o invasor pode transmitir um servidor que pode ser aceito pelos usuários.

A configuração padrão do firewall mostrada na caixa de diálogo da proposta é rejeitar transmissões IPP em qualquer interface. Da mesma forma, o segundo método para detecção de filas remotas e o terceiro método para acesso de filas remotas não funcionarão. Portanto, a configuração do firewall deve ser modificada marcando-se uma das interfaces como `interna`, que abre a porta por padrão, ou abrindo-se explicitamente a porta de uma interface `externa`. Por motivos de segurança, nenhuma porta é aberta por padrão.

A configuração de firewall proposta deve ser modificada para habilitar o CUPS a detectar filas remotas durante a instalação e acessar servidores remotos do sistema local durante a operação normal. O usuário também pode detectar os servidores CUPS verificando ativamente os hosts de rede locais ou configurar filas manualmente. No entanto, por causa das razões mencionadas no início desta seção, esse método não é recomendado.

31.6.2 Mudanças no serviço de impressão do CUPS

Estas mudanças foram inicialmente aplicadas para o SUSE Linux 9.1.

Execuções de cupsd como usuário lp

Na inicialização, `cupsd` muda do usuário `root` para o usuário `lp`. Isso oferece um nível de segurança muito maior porque o serviço de impressão CUPS não é executado com permissões irrestritas, mas somente com as permissões necessárias para o serviço de impressão.

Entretanto, a autenticação (a verificação de senha) não pode ser executada via /etc/shadow, porque lp não tem acesso a /etc/shadow. Em vez disso, deve ser usada a autenticação específica do CUPS via /etc/cups/passwd.md5. Para esses fins, o administrador do CUPS com o grupo de administração do CUPS sys e a senha do CUPS devem ser digitados em /etc/cups/passwd.md5. Para isso, digite o seguinte como root:

```
lppasswd -g sys -a CUPS-admin-name
```

Esta configuração também é essencial se você quiser usar o front end da Web de administração (CUPS) ou a ferramenta de administração da impressora (KDE).

Quando cupsd é executado como lp, /etc/printcap não pode ser gerado, porque lp não pode criar arquivos em /etc/. Portanto, cupsd gera /etc/cups/printcap. Para assegurar que os aplicativos que lêem somente nomes de fila de /etc/printcap continuem a funcionar adequadamente, /etc/printcap é um link simbólico que aponta para /etc/cups/printcap.

Quando cupsd é executado como lp, a porta 631 não pode ser aberta. Portanto, cupsd não pode ser recarregado com rccups reload. Use rccups restart.

Funcionalidade genérica para BrowseAllow e BrowseDeny

As permissões de acesso para BrowseAllow e BrowseDeny se aplicam a todos os tipos de pacotes enviados para cupsd. As configurações padrão em /etc/cups/cupsd.conf são as seguintes:

```
BrowseAllow @LOCAL
BrowseDeny All
```

e

```
<Local />
 Order Deny,Allow
 Deny From All
 Allow From 127.0.0.1
 Allow From 127.0.0.2
 Allow From @LOCAL
 </Local>
```

Dessa forma, somente hosts LOCAL podem acessar cupsd em um servidor CUPS. Hosts LOCAL são hosts cujos endereços IP pertencem a uma interface não-PPP

(interfaces cujos sinalizadores IFF_POINTOPOINT não estão definidos) e pertencem à mesma rede do servidor CUPS. Pacotes de todos os outros hosts serão rejeitados imediatamente.

cupsd ativado por padrão

Em uma instalação padrão, cupsd é ativado automaticamente, permitindo fácil acesso a filas de servidores de rede CUPS sem qualquer ação manual adicional. Os itens em "Execuções de cupsd como usuário lp" (p 503) e "Funcionalidade genérica para BrowseAllow e BrowseDeny" (p 504) são pré-condições essenciais desse recurso, caso contrário a segurança não seria suficiente para ativação automática de cupsd.

31.6.3 Arquivos PPD em pacotes diferentes

A configuração de impressora do YaST define as filas do CUPS usando apenas os arquivos PPD instalados em /usr/share/cups/model/ no sistema. Para localizar os arquivos PPD adequados ao modelo de impressora, o YaST compara o fabricante e o modelo determinados durante a detecção do hardware aos fabricantes e modelos de todos os arquivos PPD disponíveis em /usr/share/cups/model/ no sistema. Para isso, a configuração de impressora do YaST gera um banco de dados com as informações de fabricante e modelo extraídas dos arquivos PPD. Quando você seleciona uma impressora na lista de fabricantes e modelos, recebe os arquivos PPD que correspondem ao fabricante e modelo adequados.

A configuração usando apenas arquivos PPD e nenhuma outra fonte de informação tem a vantagem de permitir a livre modificação de arquivos PPD em /usr/share/cups/model/. A configuração de impressora do YaST reconhece as mudanças e gera novamente o banco de dados de fabricantes e modelos. Por exemplo, se você tem apenas impressoras PostScript, normalmente não precisa dos arquivos PPD Foomatic do pacote cups-drivers ou os arquivos PPD Gimp-Print do pacote cups-drivers-stp. Em vez disso, os arquivos PPD de suas impressoras PostScript podem ser copiados diretamente para /usr/share/cups/model/ (se já não existem no pacote manufacturer-PPDs) para que você obtenha uma configuração ideal para suas impressoras.

Arquivos PPD do CUPS do pacote `cups`

Os arquivos PPD genéricos do pacote `cups` foram complementados com arquivos PPD Foomatic adaptados para impressoras PostScript nível 1 e 2:

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

Arquivos PPD do pacote `cups-drivers`

Normalmente, o filtro de impressora Foomatic `foomatic-rip` é usado junto com Ghostscript para impressoras não-PostScript. Os arquivos PPD Foomatic adequados têm as entradas `*NickName: ... Foomatic/Ghostscript driver` e `*cupsFilter: ... foomatic-rip`. Esses arquivos PPD estão localizados no pacote `cups-drivers`.

O YaST preferirá um arquivo PPD Foomatic se um arquivo destes com a entrada `*NickName: ... Foomatic ... (recommended)` corresponder ao modelo de impressora e o pacote `manufacturer-PPDs` não contiver um arquivo PPD mais adequado.

Arquivos PPD Gimp-Print do pacote `cups-drivers-stp`

Em vez de `foomatic-rip`, o filtro CUPS `rastertoprinter` do Gimp-Print pode ser usado em várias impressoras não-PostScript. Esse filtro e os arquivos PPD Gimp-Print adequados estão disponíveis no pacote `cups-drivers-stp`. Os arquivos PPD Gimp-Print estão localizados em `/usr/share/cups/model/stp/` e têm as entradas `*NickName: ... CUPS+Gimp-Print` e `*cupsFilter: ... rastertoprinter`.

Arquivos PPD de fabricantes de impressoras no pacote `manufacturer-PPDs`

O pacote `manufacturer-PPDs` contém arquivos PPD de fabricantes de impressoras que são liberados mediante uma licença suficientemente permissiva. Impressoras

PostScript devem ser configuradas com o arquivo PPD adequado do fabricante da impressora, já que esse arquivo permite o uso de todas as funções da impressora PostScript. O YaST preferirá um arquivo PPD do pacote `manufacturer-PPDs` se as seguintes condições forem atendidas:

- O fabricante e o modelo determinados durante a detecção do hardware correspondem ao fabricante e ao modelo de um arquivo PPD do pacote `manufacturer-PPDs`.

- O arquivo PPD do pacote `manufacturer-PPDs` é o único arquivo PPD adequado para o modelo de impressora ou existe um arquivo PPD Foomatic com uma entrada `*NickName: ... Foomatic/Postscript (recommended)` que também corresponde ao modelo de impressora.

Assim, o YaST não usa nenhum arquivo PPD do pacote `manufacturer-PPDs` nos seguintes casos:

- O arquivo PPD do pacote `manufacturer-PPDs` não corresponde ao fabricante e ao modelo. Isso poderá ocorrer se o pacote `manufacturer-PPDs` contiver apenas um arquivo PPD para modelos semelhantes, por exemplo, se não houver arquivo PPD separado para os modelos individuais de uma série de modelos, mas o nome do modelo for especificado na forma `Funprinter 1000 series` no arquivo PPD.

- O arquivo PPD Foomatic PostScript não é recomendado. Isso talvez ocorra porque o modelo de impressora não funciona suficientemente bem no modo PostScript; por exemplo, a impressora pode não ser confiável nesse modo porque tem pouca memória ou é muito lenta porque seu processador é fraco. Além disso, a impressora pode não suportar PostScript por padrão porque, por exemplo, o suporte a PostScript só está disponível como módulo opcional.

Se um arquivo PPD do pacote `manufacturer-PPDs` for adequado para uma impressora PostScript, mas o YaST não puder configurá-lo por esses motivos, selecione manualmente o modelo de impressora respectivo no YaST.

31.7 Solução de problemas

As seções a seguir abordam alguns dos problemas mais encontrados em relação a hardware e software de impressora, bem como formas de solucionar ou superar esses problemas.

31.7.1 Impressoras sem suporte de linguagem de impressora padrão

As impressoras que não suportam nenhuma linguagem de impressora comum e só podem ser endereçadas com seqüências de controle especiais são chamadas de *impressoras GDI*. Essas impressoras só funcionam com as versões do sistema operacional para as quais o fabricante oferece driver. *GDI* é uma interface de programação desenvolvida pela Microsoft para dispositivos gráficos. O verdadeiro problema não é a interface de programação, mas o fato de que as impressoras GDI só podem ser endereçadas com a linguagem de impressora proprietária do respectivo modelo de impressora.

Algumas impressoras podem ser modificadas para funcionar no modo GDI ou em uma das linguagens de impressora padrão. Alguns fabricantes oferecem drivers proprietários para suas impressoras GDI. A desvantagem dos drivers de impressora proprietários é que não há garantia de que vão funcionar com o sistema de impressão instalado e de que são adequados para as diferentes plataformas de hardware. Em contraste, impressoras que suportam uma linguagem de impressora padrão não dependem de uma versão do sistema de impressão especial ou de plataforma de hardware especial.

Em vez de desperdiçar tempo tentando fazer um driver Linux proprietário funcionar, pode ser mais eficaz comprar uma impressora suportada. Isso solucionaria o problema do driver de uma vez por todas, eliminando a necessidade de instalar e configurar software de driver especial e obter atualizações do driver eventualmente necessárias devido a novos avanços no sistema de impressão.

31.7.2 Nenhum arquivo PPD adequado disponível para impressora PostScript

Se o pacote `manufacturer-PPDs` não contiver qualquer arquivo PPD adequado para uma impressora PostScript, será possível usar o arquivo PPD do CD do driver do fabricante da impressora ou fazer download de um arquivo PPD adequado da página da Web do fabricante.

Se o arquivo PPD for fornecido como arquivo compactado (.zip) ou arquivo compactado de auto-extração (`.exe`), faça a descompactação com `unzip`. Primeiro, reveja os termos de licença do arquivo PPD. Use o utilitário `cupstestppd` para verificar se o arquivo PPD é compatível com a "Especificação de Formato do Arquivo de Descrição de Impressora Adobe PostScript, versão 4.3". Se o utilitário retornar "FAIL", os erros dos arquivos PPD são sérios e provavelmente causarão grandes problemas. Os problemas reportados pelo `cupstestppd` devem ser eliminados. Se necessário, peça o arquivo PPD adequado ao fabricante da impressora.

31.7.3 Portas paralelas

A abordagem mais segura é conectar a impressora diretamente à primeira porta paralela e selecionar as configurações de porta paralela no BIOS:

- Endereço de E/S: `378` (hexadecimal)
- Interrupção: irrelevante
- Modo: `Normal`, `SPP` ou `Output Only`
- DMA: desabilitado

Se a impressora não puder ser endereçada na porta paralela apesar dessas configurações, digite o endereço de E/S explicitamente de acordo com a configuração no BIOS no formato `0x378` em `/etc/modprobe.conf`. Se houver duas portas paralelas definidas para os endereços de E/S `378` e `278` (hexadecimal), digite-os no formato `0x378,0x278`.

Se a interrupção `7` estiver livre, poderá ser ativada com a entrada mostrada em Exemplo 31.1, "/etc/modprobe.conf: Modo de interrupção para a primeira porta paralela" (p 510). Antes de ativar o modo de interrupção, verifique o arquivo `/proc/interrupts` para ver quais interrupções já estão sendo usadas. Somente as interrupções usadas atualmente são exibidas. Isso pode mudar dependendo dos componentes de hardware ativos. A interrupção da porta paralela não deve ser usada por outro dispositivo. Se não tiver certeza, use o modo de polling com `irq=none`.

Exemplo 31.1 */etc/modprobe.conf: Modo de interrupção para a primeira porta paralela*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

31.7.4 Conexões da impressora de rede

Identificação de problemas de rede

Conecte a impressora diretamente ao computador. Para fins de teste, configure-a como impressora local. Se isso funcionar, o problema está na rede.

Verificando a rede TCP/IP

A rede TCP/IP e a resolução de nomes devem ser funcionais.

Verificando um `lpd` remoto

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com `lpd` (porta `515`) no *`host`*.

```
netcat -z host 515 && echo ok || echo failed
```

Se a conexão com `lpd` não for estabelecida, o `lpd` pode não estar ativo ou pode haver problemas básicos de rede.

Como usuário `root`, use o seguinte comando para consultar um relatório de status (possivelmente muito longo) sobre a *`fila`* no *`host`* remoto, considerando que o respectivo `lpd` esteja ativo e o host aceite consultas:

```
echo -e "\004queue" \
| netcat -w 2 -p 722 host 515
```

Se o `lpd` não responder, ele pode não estar ativo ou pode haver problemas básicos de rede. Se o `lpd` responder, a resposta deve mostrar por que não é possível imprimir na `fila` do `host`. Se você receber uma resposta como a do Exemplo 31.2, "Mensagem de erro do `lpd`" (p 510), o problema está sendo causado pelo `lpd` remoto.

Exemplo 31.2 *Mensagem de erro do lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Verificando um `cupsd` remoto

Por padrão, o servidor de rede CUPS deve transmitir suas filas a cada 30 segundos na porta UDP `631`. Por isso, o seguinte comando pode ser usado para testar a existência de um servidor de rede CUPS na rede.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Se existir um servidor de rede CUPS de transmissão, a saída aparecerá conforme mostrado no Exemplo 31.3, “Transmissão do servidor de rede CUPS” (p 511).

Exemplo 31.3 *Transmissão do servidor de rede CUPS*

```
ipp://host.domain:631/printers/queue
```

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com `cupsd` (porta `631`) no *`host`*.

```
netcat -z host 631 && echo ok || echo failed
```

Se a conexão com `cupsd` não for estabelecida, o `cupsd` pode não estar ativo ou existem problemas básicos de rede. `lpstat -h host -l -t` retorna um relatório de status (possivelmente muito longo) para todas as filas do *`host`*, desde que o respectivo `cupsd` esteja ativo e o host aceite consultas.

O próximo comando pode ser usado para testar se a *`fila`* do *`host`* aceita uma tarefa de impressão consistindo em um único caractere de retorno de carro. Nada será impresso. Possivelmente, será ejetada uma página em branco.

```
echo -en "\r" \
  | lp -d fila -h host
```

Solução de problemas da impressora de rede ou da caixa do servidor de impressão

Algumas vezes, spoolers executados na caixa do servidor de impressão causam problemas quando precisam lidar com muitas tarefas de impressão. Como isso é causado pelo spooler nessa caixa, não há solução para o problema. Como paliativo, desvie o spooler na caixa do servidor de impressão endereçando a impressora conectada à caixa diretamente por meio do soquete TCP. Consulte a Seção 31.4.2, “Impressoras de rede” (p 498).

Dessa forma, a caixa do servidor de impressão é reduzida a um conversor entre as várias formas de transferência de dados (conexão de rede TCP/IP e impressora local). Para usar esse método, você precisa conhecer a porta TCP da caixa do servidor de impressão. Se a impressora estiver conectada à caixa do servidor de impressão e ligada, a porta TCP poderá, geralmente, ser determinada com o utilitário `nmap`

do pacote `nmap` depois que essa caixa for ativada. Por exemplo, `nmap`*`endereço IP`* pode resultar na seguinte saída para a caixa do servidor de impressão:

```
Port        State       Service
23/tcp      open        telnet
80/tcp      open        http
515/tcp     open        printer
631/tcp     open        cups
9100/tcp    open        jetdirect
```

Essa saída indica que a impressora conectada à caixa do servidor de impressão pode ser endereçada via soquete TCP na porta `9100`. Por padrão, `nmap` verifica somente algumas portas mais conhecidas listadas em `/usr/share/nmap/nmap-services`. Para verificar todas as portas possíveis, use o comando `nmap -p`*`porta_de_origem-porta_de_destino endereço-IP`*. O processo pode demorar. Para obter mais informações, consulte a página de manual `nmap`.

Digite um comando como

```
echo -en "\rHello\r\f" | netcat -w 1 porta endereço-IP arquivo
cat | netcat -w 1 porta endereço-IP
```

para enviar strings de caracteres ou arquivos diretamente à respectiva porta para testar se a impressora pode ser endereçada dessa porta.

31.7.5 Defeitos na impressão sem mensagem de erro

Para o sistema de impressão, a tarefa de impressão é concluída quando o back end do CUPS finaliza a transferência de dados ao destinatário (impressora). Se houver falha no processamento posterior no destinatário (por exemplo, se a impressora não imprimir seus dados específicos), o sistema de impressão não notará. Se a impressora não imprimir seus dados específicos, selecione outro arquivo PPD mais adequado à impressora.

31.7.6 Filas desabilitadas

Se a transferência de dados para o destinatário falhar completamente após várias tentativas, o back end do CUPS, como `usb` ou `soquete`, reportará um erro ao sistema de impressão (ao `cupsd`). O back end decide se e quantas tentativas devem ser feitas

até que a transferência de dados seja reportada como impossível. Como tentativas posteriores podem ser inúteis, o `cupsd` desabilita a impressão da fila respectiva. Após eliminar a causa do problema, o administrador do sistema deve reabilitar a impressão com o comando `/usr/bin/enable`.

31.7.7 Navegação no CUPS: apagando tarefas de impressão

Se um servidor de rede CUPS transmitir suas filas aos hosts de clientes via navegação e um `cupsd` local adequado estiver ativo nos hosts de clientes, o `cupsd` cliente aceitará tarefas de impressão de aplicativos e as encaminhará para o `cupsd` no servidor. Quando o `cupsd` aceita uma tarefa de impressão, esta recebe um novo número. Portanto, o número da tarefa no host cliente é diferente do número da tarefa no servidor. Como geralmente a tarefa de impressão é encaminhada de imediato, não pode ser apagada com o número de tarefa do host cliente, porque o `cupsd` cliente considera a tarefa como concluída assim que ela é encaminhada ao `cupsd` do servidor.

Para apagar a tarefa de impressão no servidor, use um comando como `lpstat –h servidor-de-impress o –o` para determinar o número da tarefa no servidor, contanto que o servidor não tenha concluído a tarefa de impressão (isto é, enviado para a impressora). Usando este número, a tarefa de impressão pode ser apagada no servidor:

```
cancel -h servidor-de-impress o fila-nr_taref
```

31.7.8 Tarefas de impressão defeituosas e erros de transferência de dados

As tarefas de impressão permanecerão nas filas e a impressão recomeçará se você desligar e ligar a impressora ou desligar e reinicializar o computador durante o processo de impressão. As tarefas de impressão defeituosas devem ser removidas da fila com `cancel`.

Se a tarefa de impressão apresentar defeito ou se ocorrer um erro na comunicação entre o host e a impressora, a impressora imprimirá várias folhas de papel com caracteres ininteligíveis porque não conseguiu processar os dados corretamente. Para solucionar esse problema, siga este procedimento:

1. Para interromper a impressão, remova todo o papel das bandejas da impressora jato de tinta ou laser. Impressoras de alta qualidade têm um botão de cancelamento da impressão.

2. A tarefa de impressão pode ainda estar na fila, já que as tarefas são removidas somente depois de enviadas completamente à impressora. Use `lpstat -o` ou `lpstat -h` *`servidor-de-impressão`* `-o` para verificar a fila que está sendo impressa. Apague a tarefa com `cancel` *`fila-númerodatarefa`* ou `cancel -h` *`servidor-de-impressão fila-númerodatarefa`*.

3. Alguns dados podem ainda ser transferidos à impressora mesmo que a tarefa seja apagada da fila. Verifique se há um processo back end do CUPS em execução para a fila respectiva e termine-o. Por exemplo, para uma impressora conectada à porta paralela, o comando `fuser -k /dev/lp0` pode ser usado para terminar todos os processos que ainda estão acessando a impressora (mais precisamente: a porta paralela).

4. Reinicialize a impressora completamente deixando-a desligada por um tempo. Em seguida, insira o papel e ligue a impressora.

31.7.9 Depuração do sistema de impressão do CUPS

Use o seguinte procedimento genérico para localizar problemas no sistema de impressão do CUPS:

1. Defina `LogLevel debug` em `/etc/cups/cupsd.conf`.

2. Pare o `cupsd`.

3. Remova `/var/log/cups/error_log*` para não precisar procurar em arquivos de registro muito grandes.

4. Inicie o `cupsd`.

5. Repita a ação que causou o problema.

6. Verifique as mensagens em `/var/log/cups/error_log*` para identificar a causa do problema.

31.7.10 Mais informações

Soluções para vários problemas específicos são apresentadas no Banco de Dados de Suporte. Em caso de problemas com a impressora, consulte os artigos do Banco de Dados de Suporte *Installing a Printer* e *Printer Configuration from SUSE Linux 9.2*, que você pode procurar com a palavra-chave *printer*.

32 O sistema hotplug

O sistema hotplug controla a inicialização da maioria dos dispositivos em um computador. Ele não é usado para dispositivos que podem ser inseridos e removidos durante a operação, mas para todos os dispositivos detectados enquanto o sistema está inicializando. Ele trabalha junto com o sistema de arquivos `sysfs` e `udev`, que estão descritos em Capítulo 33, *Nós de dispositivo dinâmicos com* `udev` (p 525).

Até que o kernel tenha sido inicializado, somente dispositivos que são absolutamente necessários, como o sistema de barramento, discos de inicialização e teclado, são inicializados. O kernel aciona eventos hotplug para todos os dispositivos detectados. O daemon `udevd` ouve esses eventos e executa o `udev` para criar o nó de dispositivos e configurar o dispositivo. Para dispositivos que não podem ser detectados automaticamente, como cartões ISA antigos, uma configuração estática é utilizada.

Fora algumas exceções históricas, a maioria dos dispositivos é inicializada imediatamente assim que estão acessíveis, durante a inicialização do sistema ou quando os dispositivos estão conectados por hotplug. Durante a inicialização, as interfaces são registradas com o kernel. Este registro aciona mais eventos hotplug que causam uma configuração automática da respectiva interface.

Em versões anteriores do SUSE Linux, um conjunto estático de dados de configuração era usado como a base para os dispositivos de inicialização. Quaisquer eventos hotplug eram tratados por scripts separados, chamados agentes. Com este lançamento do SUSE Linux, o subsistema hotplug é integrado ao udev, com udev, as regras fornecem a funcionalidade dos antigos agentes hotplug.

As configurações gerais para o subsistema hotplug podem ser encontradas em `/etc/sysconfig/hotplug`. Todas as variáveis são comentadas. A configuração geral

do dispositivo é realizada dependendo de regras correspondentes encontradas em `/etc/udev/rules.d` (consulte Capítulo 33, *Nós de dispositivo dinâmicos com* `udev` (p 525)). Arquivos de configuração para dispositivos específicos estão localizados em `/etc/sysconfig/hardware`. A rechamada do evento hotplug usada na versão anterior do SUSE Linux, `/proc/sys/kernel/hotplug`, é geralmente vazia pois `udevd` recebe mensagens hotplug através de um soquete de netlink.

32.1 Dispositivos e interfaces

O sistema hotplug configura dispositivos e interfaces. Um dispositivo é em geral conectado a um barramento e fornece a funcionalidade necessária para uma interface. Uma interface representa a abstração visível ao usuário de todo o dispositivo ou de um determinado subconjunto. Um dispositivo em geral exige um driver de dispositivos na forma de módulos de kernel para funcionar de forma adequada. Além disso, algum driver e nível superior pode ser necessário para fornecer a interface ao usuário. Interfaces são em geral representadas por nós de dispositivo criados por `udev`. A distinção entre dispositivos e interfaces é importante para compreender o conceito geral.

Dispositivos inseridos no sistema de arquivos `sysfs` são encontrados sob `/sys/devices`. Interfaces estão localizadas sob `/sys/class` ou `/sys/block`. Todas as interfaces em `sysfs` devem ter um link a seus dispositivos. Porém, há ainda alguns drivers que não são adicionados automaticamente a este link. Sem este link, não é possível saber a qual dispositivo pertence esta interface e uma configuração adequada não poderá ser localizada.

Dispositivos tratados através de uma descrição de dispositivo. Esse pode ser o caminho do dispositivo em `sysfs` (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`), uma descrição do ponto de conexão (`bus-pci-0000:02:00.0`), um ID individual (`id-32311AE03FB82538`), ou algo similar. No passado, interfaces eram tratadas através de seus nomes. Esses nomes representavam uma numeração simples dos dispositivos existentes e pode ter sido alterada quando dispositivos foram adicionados ou removidos.

Interfaces também podem ser tratadas através de uma descrição do dispositivo associado. Em geral, o contexto indica se a descrição refere-se ao próprio dispositivo ou à sua interface. Exemplos típicos de dispositivos, interfaces e descrições incluem:

Placa de rede PCI
Um dispositivo que é conectado ao barramento PCI (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` ou `bus-pci-0000:02:00.0`) e tem uma interface de rede (`eth0`, `id-00:0d:60:7f:0b:22` ou `bus-pci-0000:02:00.0`). A interface de rede é usada por serviços de rede ou conectada a um dispositivo de rede virtual, como um túnel ou VLAN, que por sua vez tem uma interface.

Controlador PCI SCSI
Um dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` ou `bus-scsi-1:0:0:0`) que torna disponíveis várias interfaces físicas na forma de um barramento (`/sys/class/scsi_host/host1`).

Disco rígido SCSI
Um dispositivo (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0` ou `bus-scsi-1:0:0:0`) com várias interfaces (`/sys/block/sda*`).

32.2 Eventos hotplug

Cada dispositivo e cada interface tem um *evento hotplug* associado, que é processado por `udev`. Eventos hotplug são acionados pelo kernel quando um link a um dispositivo é estabelecido ou removido ou quando um driver registra ou exclui uma interface. Desde o SUSE Linux 9.3, o `udevd` recebe e processa eventos hotplug. O `udevd` ouve diretamente mensagens de netlink do kernel ou `/sbin/udevsend` deve ser especificado em `/proc/sys/kernel/hotplug`. `udevd` configura o dispositivo de acordo com um conjunto de regras (consulte Capítulo 33, *Nós de dispositivo dinâmicos com* `udev` (p 525)).

32.3 Configuração do dispositivo hotplug

Agentes hotplug foram desaprovados a partir do SUSE Linux 10.0. Toda a configuração de dispositivos agora deve ser realizada via regras de udev. `udev` fornece uma regra

de compatibilidade para chamar agentes personalizados existentes. Porém, converter agentes personalizados em regras udev deve ser considerado.

Um agente hotplug é um programa executável que executa ações adequadas para um evento. Os agentes para os eventos de dispositivo estão localizados em `/etc/hotplug.d/`*`nome do evento`* e `/etc/hotplug.d/default`. Todos os programas nesses diretórios com o sufixo `.hotplug` são executados em ordem alfabética.

Para facilitar a configuração do dispositivo, em geral é suficiente carregar um módulo de kernel. Em alguns casos, comandos adicionais precisam ser chamados para uma configuração de dispositivo adequada. No SUSE Linux, isso é tratado geralmente por regras de udev. Porém, se uma configuração de dispositivo personalizada é necessária, a configuração do dispositivo é realizada por `/sbin/hwup` ou `/sbin/hwdown`. Esses programas procuram uma configuração adequada para o dispositivo no diretório `/etc/sysconfig/hardware` e a aplicam. Por exemplo, para evitar que um dispositivo específico seja inicializado, crie um arquivo de configuração com um nome apropriado e defina o modo de inicialização para `manual` ou `off`. Se `/sbin/hwup` não encontrar qualquer configuração, ele procura pela variável de ambiente `MODALIAS`. Se ela existir, `modprobe` automaticamente carrega o módulo correspondente. A variável `MODALIAS` é gerada automaticamente por eventos hotplug do kernel para dispositivos que exigem um módulo para serem carregados. Para obter mais informações, consulte Seção 32.4, “Carregamento de módulo automático” (p 522). Mais informações sobre `/sbin/hwup` estão disponíveis no arquivo `/usr/share/doc/packages/sysconfig/README` e na página de manual `man hwup`.

Antes de agentes de interface serem chamados, `udev` geralmente gera um nó de dispositivo que o sistema pode acessar. `udev` permite a atribuição de nomes persistentes a interfaces. Consulte Capítulo 33, *Nós de dispositivo dinâmicos com* `udev` (p 525) para obter detalhes. Em seguida, as próprias interfaces são configuradas de acordo com as regras de udev respectivas. Os procedimentos para algumas interfaces estão descritos abaixo.

32.3.1 Ativando interfaces de rede

Interfaces de rede são inicializadas com `/sbin/ifup` e desativadas com `/sbin/ifdown`. Detalhes são fornecidos no arquivo `/usr/share/doc/packages/sysconfig/README` e na página de manual `ifup`.

Se um computador tem vários dispositivos de rede com drivers diferentes, as designações da interface podem ser alteradas se outro driver for carregado de forma mais rápida enquanto o sistema está inicializando. O SUSE Linux tenta manter a numeração persistente—os dispositivos mantêm o nome de interface ao qual foram atribuídos durante a configuração. A atribuição é realizada via regras de udev. Para alterar a atribuição posteriormente, as regras de udev devem ser alteradas.

Porém, a melhor solução é usar as designações de interface persistentes. Você pode especificar os nomes das interfaces individuais nos arquivos de configuração. Detalhes sobre este método estão disponíveis no arquivo `/usr/share/doc/packages/sysconfig/README`. Desde o SUSE Linux 9.3, o udev também lida com interfaces de rede, embora estes não sejam nós de dispositivo. Isso permite o uso de nomes de interface persistentes de forma mais padronizada.

32.3.2 Ativando dispositivos de armazenamento

Interfaces para armazenar dispositivos devem ser montadas para que seja possível acessá-las. Isso pode ser totalmente automatizado ou pré-configurado. Além disso, o SUSE Linux distingue entre dispositivos de usuário e sistema. Dispositivos de sistema só podem ser montados automaticamente através da criação de uma entrada em `/etc/fstab`. Dispositivos de usuário são tratados via `hal` por padrão. Se uma configuração diferente para dispositivos de usuário for necessária, esses dispositivos podem ser inseridos em `/etc/fstab`. Alternativamente, o tratamento deste dispositivo em `hal` pode ser modificado. Para obter mais informações sobre `hal`, consulte `/usr/share/doc/packages/hal/hal-spec.html`.

O uso de nomes de dispositivos persistentes é recomendado, pois nomes de dispositivos tradicionais podem ser alterados, dependendo da seqüência de inicialização. Detalhes sobre nomes de dispositivos persistentes estão disponíveis em Capítulo 33, *Nós de dispositivo dinâmicos com* `udev` (p 525).

32.4 Carregamento de módulo automático

Se /sbin/hwup falhar em detectar um arquivo de configuração, modprobe procurará um módulo correspondente baseado no conteúdo da variável de ambiente MODALIAS. Essa variável de ambiente é gerada pelo kernel para o evento hotplug correspondente. Para usar um driver diferente do padrão para o kernel, um arquivo de configuração de hardware apropriado em /etc/sysconfig/hardware deve ser criado.

32.5 O Script de boot coldplug

boot.coldplug é responsável pela inicialização de todos os dispositivos que não foram configurados durante a inicialização. Ele chama hwup para toda configuração de dispositivo estática designada como /etc/sysconfig/hardware/hwcfg-static-*. Após, ele repete todos os eventos armazenados em /lib/klibc/events para inicializar todos os dispositivos.

32.6 Análise de erro

32.6.1 Arquivos de registro

A menos que especificado de outra forma, hotplug envia somente algumas mensagens importantes para syslog. Para obter mais informações, defina a variável HOTPLUG_DEBUG no arquivo /etc/sysconfig/hotplug para yes. Se você definir esta variável para o valor max, todo comando shell será registrado para scripts de hotplug. Isso significa que /var/log/messages nas quais syslog armazena todas as mensagens torna-se bem maior. Como syslog é iniciado durante o processo de inicialização após hotplug e coldplug, é possível, porém, que as primeiras mensagens não sejam registradas. Se essas mensagens forem importantes para você, especifique um arquivo de registro via a variável HOTPLUG_SYSLOG. Informações sobre este tópico estão disponíveis em /etc/sysconfig/hotplug.

32.6.2 Problemas de inicialização

Se um computador desligar durante o processo de inicialização, desative `hotplug` ou `coldplug` digitando `NOHOTPLUG=yes` ou `NOCOLDPLUG=yes` no prompt de inicialização. Devido à desativação do hotplug, o kernel não emite quaisquer eventos hotplug. No sistema em execução, você pode ativar o hotplug digitando o comando `/etc/init.d/boot.hotplug start`. Todos os eventos gerados até o momento são emitidos e processados. Para rejeitar os eventos na fila, primeiro digite `/bin/true` em `/proc/sys/kernel/hotplug` e redefina a entrada para `/sbin/hotplug` após algum tempo. Devido à desativação do coldplug, as configurações estáticas não são aplicadas. Para aplicar as configurações estáticas, digite posteriormente `/etc/init.d/boot.coldplug start`.

Para descobrir se um módulo específico carregado por `hotplug` é responsável pelo problema, digite `HOTPLUG_TRACE=<N>` no prompt de inicialização. Os nomes de todos os módulos a serem carregados são então listados na tela antes de serem realmente carregados após *N* segundos. Você não pode intervir enquanto isto estiver ocorrendo.

32.6.3 O gravador de eventos

O script `/sbin/hotplugeventrecorder` é executado para cada evento por uma regra de udev. Se um diretório `/events` existir, todos os eventos hotplug são armazenados como arquivos individuais neste diretório. Desta forma, eventos podem ser regenerados para propósitos de teste. Se este diretório não existir, nada será registrado.

Nós de dispositivo dinâmicos com udev

33

O kernel 2.6 do Linux introduz uma nova solução de espaço do usuário para um diretório de dispositivos dinâmicos `/dev` com designações de dispositivo persistentes: `udev`. Ele fornece somente os arquivos para dispositivos que estejam realmente presentes. Ele cria ou remove arquivos de nós de dispositivo geralmente localizados no diretório `/dev` e é capaz de renomear interfaces do usuário. A implementação anterior de um `/dev` dinâmico com `devfs` foi substituída pelo `udev`.

Tradicionalmente, os nós de dispositivo eram armazenados no diretório `/dev` nos sistemas Linux. Havia um nó para cada tipo possível de dispositivo, independentemente de se ele realmente existia no sistema. Como resultado, este diretório continha milhares de arquivos não usados. Antes de que um subsistema adicionado ou dispositivo de kernel fosse utilizável, os nós correspondentes precisavam ser criados com um aplicativo especial. O sistema de arquivos `devfs` trouxe uma melhora significante, porque somente os dispositivos que realmente existiam e eram conhecidos pelo kernel receberam um nó de dispositivo em `/dev`.

O `udev` introduz uma nova maneira de criar nós de dispositivo. O kernel exporta seu estado interno no `sysfs` e, cada vez que um dispositivo é reconhecido pelo kernel, ele atualiza as informações no `sysfs` e envia um evento ao espaço do usuário. Com as informações disponibilizadas pelo `sysfs`, o udev corresponde a uma sintaxe de regras simples com os atributos do dispositivo fornecidos e cria ou remove os nós de dispositivo correspondentes.

O usuário não precisa criar uma regra udev para novos dispositivos. Se o dispositivo estiver conectado, o nó de dispositivo apropriado será criado automaticamente. No entanto, as regras introduzem a possibilidade de definir uma política de nomeação de dispositivos. Isso também oferece a conveniência de substituir um nome de dispositivo

enigmático por um nome que seja fácil de lembrar e também de ter nomes de dispositivo persistentes onde dois dispositivos do mesmo tipo foram conectados ao mesmo tempo.

Pressuponha que você tenha duas impressoras, uma impressora a laser em cores de alta qualidade e uma impressora de jato de tinta em preto e branco, ambas conectadas através do USB. Elas aparecem como `/dev/usb/lpX`, onde X é um número dependendo da ordem na qual elas foram conectadas. Usando o udev, crie regras udev personalizadas nomeando uma impressora `/dev/colorlaser` e a outra `/dev/inkprinter`. Como esses nós de dispositivo são criados pelo udev com base nas características do dispositivo, eles sempre apontam para o dispositivo correto, independentemente da ordem de conexão ou do status.

33.1 Criando regras

Antes de que o `udev` crie nós de dispositivo em `/dev`, ele lê todos os arquivos em `/etc/udev/rules.d` com o sufixo `.rules` em ordem alfabética. A primeira regra que se ajuste em um dispositivo será usada, mesmo que as outras regras também se apliquem. Os comentários são introduzidos com hash (#). As regras têm a seguinte forma:

```
chave, [chave,...] NOME [, LINK SIMBÓLICO]
```

Pelo menos uma chave deve ser especificada, porque são atribuídas regras a dispositivos com base nessas chaves. Também é essencial especificar um nome. O nó de dispositivo criado em `/dev` tem esse nome. O parâmetro de link simbólico opcional permite que sejam criados nós em outros locais. Uma regra para uma impressora teria a seguinte forma:

```
BUS=="usb", SYSFS{serial}=="12345", NAME="lp_hp", SYMLINK+="printers/hp"
```

Neste exemplo, existem duas chaves, `BUS` e `SYSFS{serial}`. O `udev` compara o número serial ao número serial do dispositivo que está conectado ao barramento USB. Para atribuir o nome `lp_hp` ao dispositivo no diretório `/dev`, todas as chaves devem ser idênticas. Além disso, é criado um link simbólico `/dev/printers/hp`, que se refere ao nó do dispositivo. Ao mesmo tempo, o diretório `printers` é automaticamente criado. Os trabalhos de impressão podem ser enviados ao `/dev/printers/hp` ou `/dev/lp_hp`.

33.2 Substituição de marcador

Os parâmetros NAME e SYMLINK permitem o uso de marcadores para substituir valores especiais. Um exemplo simples ilustra o procedimento:

```
BUS=="usb", SYSFS{vendor}=="abc", SYSFS{model}=="xyz", NAME="camera%n"
```

O operador %n no nome é substituído pelo número do dispositivo da câmera, como camera0 ou camera1. Outro operador útil é %k, que é substituído pelo nome do dispositivo padrão do kernel, por exemplo, hda1. Você também pode chamar um programa externo em regras udev e usar a string que é retornada nos valores NAME e SYMLINK. A lista completa de possíveis marcadores é descrita na página do manual do udev.

33.3 Correspondência de padrões em chaves

Nas chaves de regras udev, você poderá usar correspondência de padrões no estilo shell, conhecidos como curingas. Por exemplo, o caractere * pode ser usado como um marcador para quaisquer caracteres ou ? pode ser usado para precisamente um caractere arbitrário.

```
KERNEL="ts*", NAME="input/%k"
```

Esta regra atribui o nome de kernel padrão no diretório padrão a um dispositivo cuja designação começa com as letras “ts”. Encontre informações detalhadas sobre o uso de correspondência de padrões em regras udev na página do manual do udev.

33.4 Seleção de chaves

Para identificar um dispositivo exclusivamente e diferenciar vários dispositivos entre eles, uma propriedade exclusiva é essencial para um regra udev ativa. Aqui estão alguns exemplos de chaves padrão:

SUBSYSTEM
O subsistema do qual o dispositivo faz parte

BUS
O tipo de barramento de dispositivo

KERNEL
O nome do dispositivo que o kernel usa

ID
Número de dispositivo no barramento (por exemplo, ID do barramento PCI)

SYSFS{...}
atributos do dispositivo sysfs, como rótulo, fornecedor ou número serial

As chaves `SUBSYSTEM` e `ID` podem ser úteis, mas geralmente as chaves `BUS`, `KERNEL` e `SYSFS{...}` são usadas. A configuração `udev` também fornece chaves que chamam scripts externos e avaliam seus resultados. Encontre detalhes sobre isso na página do manual do `udev`.

O sistema de arquivos `sysfs` expõe informações sobre o hardware em uma árvore do diretório. Cada arquivo geralmente contém somente um item de informação, como o nome do dispositivo, o fornecedor ou o número serial. Cada um desses arquivos pode ser usado para corresponder a uma chave. Para usar várias chaves `SYSFS` em uma regra, no entanto, você pode somente usar arquivos no mesmo diretório como valores de chave. A ferramenta `udevinfo` pode ajudar a encontrar valores de chaves úteis e exclusivos.

Você deve encontrar um subdiretório de `/sys` que se refira ao dispositivo relevante e contenha um arquivo `dev`. Esses diretórios estão todos localizados sob `/sys/block` ou `/sys/class`. Se um nó de dispositivo já existir para o dispositivo, `udevinfo` poderá encontrar o subdiretório correto para você. O comando `udevinfo -q path -n /dev/sda` tem como saída `/block/sda`. Isso significa que o diretório desejado é `/sys/block/sda`. Chame agora `udevinfo` com o comando `udevinfo -a -p /sys/block/sda`. Os dois comandos também podem ser combinados, como em `udevinfo -a -p `udevinfo -q path -n /dev/sda``. A seguir está um extrato da saída:

```
BUS=="scsi"
ID=="0:0:0:0"
SYSFS{detach_state}=="0"
SYSFS{type}=="0"
SYSFS{max_sectors}=="240"
SYSFS{device_blocked}=="0"
SYSFS{queue_depth}=="1"
SYSFS{scsi_level}=="3"
```

```
SYSFS{vendor}==" "
SYSFS{model}=="USB 2.0M DSC"
SYSFS{rev}=="1.00"
SYSFS{online}=="1"
```

Nas informações de saída, procure chaves apropriadas que não mudem. Lembre-se de que você não pode usar chaves de diretórios diferentes em uma regra.

33.5 Nomes persistentes para dispositivos de armazenamento em massa

O SUSE Linux é fornecido com regras predefinidas que permitem que você sempre atribua as mesmas designações a discos rígidos e outros dispositivos de armazenamento, independentemente da ordem em que são inicializados. Os atributos de dispositivo exclusivos, como números seriais de hardware, UUIDs ou rótulos de sistema de arquivos, podem ser lidos com pequenos programas de ajuda que são fornecidos com o udev. Os programas de ajuda tornam as informações de dispositivo específicas disponíveis ao processamento de regras udev. Como um exemplo simplificado, a primeira regra importa os valores obtidos do dispositivo SCSI no ambiente udev. A segunda regra usa os valores importados a fim de criar um link simbólico persistente.

```
KERNEL="sd*[!0-9]", IMPORT="/sbin/scsi_id -g -x -s $p -d %N"
  KERNEL="sd*[!0-9]",
SYMLINK+="$env{ID_TYPE}/by-id/$env{ID_BUS}-$env{ID_SERIAL}"
```

Assim que um driver para um dispositivo de armazenamento em massa tiver sido carregado, ele registrará todos os discos rígidos disponíveis com o kernel. Cada um deles aciona um evento de bloqueio de hotplug que chama o `udev`. A seguir, o `udev` lê as regras para determinar se um link simbólico precisa ser criado.

Se o driver for carregado através do `initrd`, os eventos de hotplug serão perdidos. No entanto, todas as informações são armazenadas no `sysfs`. O utilitário `udevstart` encontra todos os arquivos de dispositivo sob `/sys/block` e `/sys/class` e inicia o `udev`.

Também existe um script de inicialização `boot.udev`, que recria todos os nós de dispositivo durante o processo de inicialização. No entanto, o script de inicialização

deve ser ativado através do editor de níveis de execução do YaST ou com o comando `insserv boot.udev`.

34 Sistemas de arquivos no Linux

O Linux suporta diversos sistemas de arquivos. Este capítulo apresenta uma breve visão geral sobre os sistemas de arquivos Linux mais populares, abordando seu conceito de design, suas vantagens e os campos de aplicação. Também são fornecidas algumas informações adicionais sobre LFS (Large File Support - Suporte a Arquivo Grande) no Linux.

34.1 Terminologia

metadados
Uma estrutura de dados interna ao sistema de arquivos que assegura que todos os dados de um disco sejam organizados adequadamente e de forma acessível. Essencialmente, tratam-se de "dados sobre os dados." Quase todo sistema de arquivos tem sua própria estrutura de metadados, razão pela qual os sistemas de arquivos exibem diferentes características de desempenho. É extremamente importante manter os metadados intactos, caso contrário todos os dados do sistema de arquivos podem se tornar inacessíveis.

inode
Inodes contêm várias informações sobre um arquivo, incluindo tamanho, número de links, data e horário da criação, da modificação e do acesso, e indicadores para os blocos de disco em que o conteúdo do arquivo está armazenado no momento.

diário
No contexto de um sistema de arquivos, o diário é uma estrutura em disco que contém um tipo de registro em que o sistema de arquivos armazena o que está prestes

a ser modificado em seus metadados. Os diários reduzem imensamente o tempo de recuperação de um sistema Linux, pois eles tornam obsoleto o extenso processo de pesquisa que verifica todo o sistema de arquivos na inicialização do sistema. Em vez disso, somente o diário é reproduzido.

34.2 Principais sistemas de arquivos no Linux

Diferentemente do que ocorria há dois ou três anos, escolher um sistema de arquivos para um sistema Linux não é mais uma questão de segundos (Ext2 ou ReiserFS?). Kernels a partir do 2.4 oferecem uma variedade de opções de sistemas de arquivos. A seguir será mostrada uma visão geral de como esses sistemas de arquivos basicamente funcionam e quais as vantagens que oferecem.

É muito importante lembrar que pode não haver um sistema de arquivos adequado a todos os tipos de aplicativos. Cada sistema de arquivos tem seus pontos fortes e fracos específicos, o que deve ser considerado. No entanto, nem mesmo o sistema de arquivos mais sofisticado pode ser substituído por uma estratégia de backup razoável.

Os termos *integridade de dados* e *consistência de dados*, quando usados neste capítulo, não se referirão à consistência dos dados do espaço do usuário (os dados que seu aplicativo grava nos arquivos). O próprio aplicativo deve controlar se os dados são consistentes ou não.

IMPORTANTE: Configurando sistemas de arquivos

A menos que declarado em outra seção deste capítulo, todas as etapas necessárias para configurar ou mudar partições em sistemas de arquivos podem ser realizadas com o módulo do YaST.

34.2.1 ReiserFS

Oficialmente um dos recursos mais importantes da versão 2.4 do kernel, o ReiserFS tornou-se disponível como um patch para kernels SUSE 2.2 x desde a versão 6.4 do SUSE Linux. O ReiserFS foi criado por Hans Reiser e pela equipe de desenvolvimento da Namesys. Ele provou ser uma alternativa robusta ao antigo Ext2. Seus bens mais

importantes são a melhor utilização do espaço em disco, o melhor desempenho do acesso ao disco e uma recuperação de falhas mais rápida.

Os pontos fortes do ReiserFS, em mais detalhes, são:

Melhor utilização do espaço em disco
No ReiserFS, todos os dados são organizados em uma estrutura chamada árvore equilibrada (B^*- tree). A estrutura de árvore contribui para uma melhor utilização do espaço em disco, pois arquivos pequenos podem ser armazenados diretamente nos nós da folha da árvore equilibrada B^*, em vez de serem armazenados em outro local e simplesmente manterem um indicador no local do disco. Além disso, o armazenamento não é alocado em pacotes de 1 ou 4 kB, mas em porções do tamanho exato necessário. Uma outra vantagem está na alocação dinâmica de inodes. Ela mantém o sistema de arquivos mais flexível do que os sistemas de arquivos tradicionais, como Ext2, em que a densidade do inode deve ser especificada no momento da criação do sistema de arquivos.

Melhor desempenho do acesso ao disco
Para arquivos pequenos, os respectivos dados e as informações (inode) "stat_data" são sempre armazenados lado a lado. Eles podem ser lidos com uma simples operação E/S de disco, o que quer dizer que é necessário somente um acesso ao disco para recuperar todas as informações necessárias.

Rápida recuperação de falhas
A utilização de um diário para controlar as mudanças de metadados recentes faz com que a verificação de um sistema de arquivos leve segundos, mesmo no caso dos muito grandes.

Confiabilidade por meio do registro dos dados em diário
O ReiserFS também suporta o registro de dados em diário e modos de dados ordenados similares aos conceitos realçados na seção Ext3, Seção 34.2.3, "Ext3" (p 534). O modo padrão é `data=ordered`, que garante a integridade dos dados e dos metadados, mas usa o registro de dados em diário somente para metadados.

34.2.2 Ext2

A origem do Ext2 remonta ao início da história do Linux. Seu predecessor, o Extended File System, foi implementado em abril de 1992 e integrado ao Linux 0.96c. O Extended File System passou por uma série de modificações e, como o Ext2, tornou-se o sistema

de arquivos Linux mais popular por muitos anos. Com a criação dos sistemas de arquivos com registro em diário e seus surpreendentes e curtos tempos de recuperação, o Ext2 ficou menos importante.

Um breve resumo dos pontos fortes do Ext2 podem ajudar a mostrar por que ele foi, e ainda é em algumas áreas, o sistema de arquivos Linux favorito de muitos usuários.

Solidez
: Por ser um “veterano,” o Ext2 passou por várias melhorias e foi bastante testado. Esta pode ser a razão para as pessoas sempre se referirem a ele como "sólido como uma pedra". Depois de uma falha no sistema em que o sistema de arquivos não pode ser desmontado inteiramente, o e2fsck começa a analisar os dados do sistema de arquivos. Os metadados são levados a um estado consistente e os arquivos pendentes ou blocos de dados são gravados em um diretório designado (chamado `lost +found`). Em contraste com os sistemas de arquivos de registro em diário, o e2fsck analisa todo o sistema de arquivos e não somente os bits de metadados modificados recentemente. Esse procedimento demora muito mais do que a verificação dos dados de registro de um sistema de arquivos com registro em diário. Dependendo do tamanho do sistema de arquivos, ele pode levar meia hora ou mais. Portanto, não é desejável optar pelo Ext2 em servidores que precisem de grande disponibilidade. No entanto, como o Ext2 não mantém um diário e usa muito menos memória, algumas vezes ele é mais rápido do que outros sistemas de arquivos.

Fácil capacidade de upgrade
: O código do Ext2 é a base sólida sobre a qual o Ext3 poderia se tornar um sistema de arquivos de última geração amplamente aclamado. Sua confiabilidade e solidez foram combinadas de forma elegante com as vantagens de um sistema de arquivos de registro em diário.

34.2.3 Ext3

O Ext3 foi criado por Stephen Tweedie. Diferentemente de todos os sistemas de arquivos de última geração, o Ext3 não segue totalmente um princípio de design novo. Ele é baseado no Ext2. Esses dois sistemas de arquivos têm uma relação muito próxima. Um sistema de arquivos Ext3 pode ser facilmente criado sobre um sistema de arquivos Ext2. A diferença mais importante entre o Ext2 e o Ext3 é que o Ext3 suporta o registro em diário. Em resumo, o Ext3 tem três grandes vantagens a oferecer:

Upgrades do Ext2 fáceis e altamente confiáveis.
Como o Ext3 é baseado no código do Ext2 e compartilha seu formato em disco, bem como seu formato de metadados, as atualizações do Ext2 para o Ext3 são incrivelmente fáceis. Diferentemente de transições para outros sistemas de arquivos de registro em diário, como o ReiserFS, o JFS e o XFS, que podem ser bastante tediosas (fazer backup de todo o sistema e recriá-lo de um rascunho), a transição para o Ext3 é uma questão de minutos. Ela também é muito segura, pois a recriação de um sistema de arquivos inteiro de um rascunho pode não ser perfeita. Considerando o número de sistemas Ext2 existentes que aguardam um upgrade para um sistema de arquivos de registro em diário, você pode imaginar facilmente por que o Ext3 pode ter alguma importância para vários administradores de sistema. O downgrade do Ext3 para o Ext2 é tão fácil quanto o upgrade. Simplesmente execute uma desmontagem completa do sistema de arquivos Ext3 e remonte-o como um sistema de arquivos Ext2.

Confiabilidade e desempenho
Alguns outros sistemas de arquivos de registro em diário seguem a abordagem de registro em diário de "Apenas Metadados". Isso significa que seus metadados são sempre mantidos em um estado consistente, mas o mesmo não pode ser garantido automaticamente para os próprios dados do sistema de arquivos. O Ext 3 foi criado para cuidar dos dados e dos metadados. O grau de "cuidado" pode ser personalizado. Habilitar o Ext3 no modo `data=journal` oferece segurança máxima (integridade de dados), mas também deixa o sistema mais lento, pois os dados e os metadados são registrados em diário. Uma abordagem relativamente nova é usar o modo `data=ordered`, que garante a integridade dos dados e metadados, mas usa o registro em diário apenas para metadados. O driver do sistema de arquivos coleta todos os blocos de dados que correspondem a uma atualização de metadados. Esses blocos de dados são gravados em disco antes da atualização dos metadados. Como resultado, obtém-se consistência para dados e metadados sem sacrificar o desempenho. Uma terceira opção é usar o `data=writeback`, para que os dados sejam gravados no mesmo sistema de arquivos depois que seus metadados forem confirmados no diário. Essa opção é sempre considerada a melhor em desempenho. Contudo, ela pode permitir que dados antigos surjam novamente nos arquivos depois de uma falha e recuperação, enquanto a integridade do sistema do arquivo é mantida. A menos que você especifique de forma diferente, o Ext3 será executado no modo `data=ordered` por padrão.

34.2.4 Convertendo um sistema de arquivos Ext2 em Ext3

A conversão do Ext2 em Ext3 envolve três etapas distintas:

Criação do diário
Efetue login como `root` e execute `tune2fs -j`. Esse procedimento criará um diário do Ext3 com os parâmetros padrão. Para que você decida o tamanho do diário e em que dispositivo ele deverá residir, execute `tune2fs -J`, juntamente com as opções de diário desejadas `size=` e `device=`. Mais informações sobre o programa tune2fs estão disponíveis em sua respectiva página de manual (tune2fs(8)).

Especificação do tipo de sistema de arquivos em /etc/fstab
Para garantir que o sistema de arquivos Ext3 seja reconhecido como tal, edite o arquivo `/etc/fstab`, mudando o tipo de sistema de arquivos especificado pela partição correspondente de `ext2` para `ext3`. A mudança terá efeito na próxima reinicialização.

Uso do Ext3 como diretório raiz
Para inicializar uma configuração de sistema de arquivos raiz como uma partição Ext3, inclua os módulos `ext3` e `jbd` no `initrd`. Para fazer isso, edite o arquivo `/etc/sysconfig/kernel` com o objetivo de incluir os dois módulos em `INITRD_MODULES`. Em seguida, execute o comando `mkinitrd`.

34.2.5 Reiser4

Logo depois que o kernel 2.6 foi lançado, a família de sistemas de arquivos com registro em diário recebeu outro membro: o Reiser4. O Reiser4 é fundamentalmente diferente de seu predecessor, o ReiserFS (versão 3.6). Ele apresenta o conceito de plug-ins para ajustar a funcionalidade do sistema de arquivos e um conceito de segurança mais refinado.

Conceito de segurança refinado
Na criação do Reiser4, seus desenvolvedores enfatizaram a implementação de recursos relevantes de segurança. Portanto, o Reiser4 contém um conjunto de plug-ins de segurança dedicados. O mais importante deles apresenta o conceito de "itens" de arquivo. Atualmente, os controles de acesso a arquivos são definidos por arquivo. Se existe um arquivo grande contendo informações relevantes para vários usuários,

grupos ou aplicativos, os direitos de acesso devem ser razoavelmente imprecisos para incluir todas as partes envolvidas. No Reiser4, é possível dividir esses arquivos em partes menores (os "itens"). Os direitos de acesso podem então ser definidos para cada item e cada usuário separadamente, permitindo um gerenciamento de segurança de arquivos muito mais preciso. Um exemplo perfeito seria `/etc/passwd`. Atualmente, somente os usuários `root` podem ler e editar o arquivo, enquanto os não-`root` só obtêm acesso de leitura a esse arquivo. Usando o conceito de item do Reiser4, você pode dividir esse arquivo em um conjunto de itens (um item por usuário) e permitir que os usuários ou aplicativos modifiquem seus próprios dados, mas sem acessar os dados de outros usuários. Esse conceito aumenta a segurança e flexibilidade.

Extensibilidade por meio de plug-ins
Muitas funções do sistema de arquivos e funções externas normalmente usadas por um sistema de arquivos são implementadas como plug-ins no Reiser4. Esses plug-ins podem ser facilmente adicionados ao sistema básico. Você não precisa mais compilar o kernel ou reformatar o disco rígido para adicionar novas funcionalidades ao sistema de arquivos.

Melhor layout do sistema de arquivos por meio de alocação atrasada
Assim como o XFS, o Reiser4 suporta a alocação atrasada. Consulte a Seção 34.2.7, "XFS" (p 538). A utilização da alocação atrasada, até mesmo para metadados, pode resultar em um melhor layout geral.

34.2.6 JFS

O JFS (*Journaling File System* - Sistema de Arquivos de Registro em Diário) foi desenvolvido pela IBM. A primeira versão beta da porta Linux JFS entrou na comunidade Linux em meados do ano 2000. A versão 1.0.0 foi lançada em 2001. O JFS foi criado para atender às necessidades de ambientes de servidores com alto throughput, em que o desempenho é a principal meta. Sendo um sistema de arquivos de 64 bits completo, o JFS suporta arquivos e partições grandes, outra razão para ele ser utilizado em ambientes de servidores.

Uma análise mais apurada do JFS mostra por que esse sistema de arquivos pode ser uma boa alternativa para seu servidor Linux:

Registro em diário eficiente

O JFS segue uma abordagem "Apenas Metadados". Em vez de uma verificação extensa, somente as mudanças dos metadados geradas por uma atividade recente do sistema de arquivos são verificadas, o que poupa muito tempo de recuperação. Operações simultâneas que requerem várias entradas de registro concorrentes podem ser combinadas em um compromisso de grupo, reduzindo imensamente a perda de desempenho do sistema de arquivos por meio de várias operações de gravação.

Organização de diretório eficiente

O JFS tem duas organizações de diretório. Para diretórios menores, ele permite que o conteúdo seja armazenado diretamente no inode. Para diretórios maiores, ele usa árvores equilibradas B^+, que facilitam muito o gerenciamento de diretório.

Melhor utilização do espaço com a alocação dinâmica do inode

No Ext2, você deve definir a densidade do inode com antecedência (o espaço ocupado pelas informações de gerenciamento), o que restringe o número máximo de arquivos ou diretórios do sistema de arquivos. O JFS o poupa dessas considerações: ele aloca dinamicamente espaço para o inode e o libera quando não é mais necessário.

34.2.7 XFS

Com intenção original de ser um sistema de arquivos para o sistema operacional IRIX, a SGI iniciou o desenvolvimento do XFS no começo de 1990. A idéia por trás do XFS era criar um sistema de arquivos de registro em diário de 64 bits de alto desempenho para atender aos altos desafios de computação de hoje. O XFS é muito bom na manipulação de arquivos grandes e tem bom desempenho em hardware de ponta. Entretanto, até mesmo o XFS tem uma desvantagem. Assim como o ReiserFS, o XFS cuida bastante da integridade dos metadados, mas nem tanto da integridade dos dados.

Uma rápida análise dos recursos fundamentais do XFS explica por que ele pode ser um forte concorrente para outros sistemas de arquivos de registro em diário em computação de ponta.

Alta escalabilidade por meio do uso de grupos de alocação

No momento de criação de um sistema de arquivos XFS, o dispositivo de bloco subjacente ao sistema de arquivos é dividido em oito ou mais regiões lineares do mesmo tamanho. Elas são denominadas *grupos de alocação*. Cada grupo de alocação gerencia seus próprios inodes e espaços liberados em disco. Praticamente, os grupos

de alocação podem ser vistos como sistemas de arquivos dentro de um sistema de arquivos. Como grupos de alocação são independentes uns dos outros, mais de um pode ser abordado pelo kernel ao mesmo tempo. Esse recurso é a chave da grande escalabilidade do XFS. Naturalmente, o conceito de grupos de alocação independente corresponde às necessidades dos sistemas com multiprocessadores.

Alto desempenho por meio de um eficiente gerenciamento de espaço em disco
O espaço em disco e os inodes são controlados por árvores equilibradas B^+ dentro dos grupos de alocação. O uso de árvores equilibradas B^+ contribui muito para o desempenho e a escalabilidade do XFS. O XFs usa a *alocação atrasada*. Ele lida com a alocação dividindo o processo em duas partes. Uma transação pendente é armazenada em RAM e o espaço necessário é reservado. O XFS ainda não decide exatamente onde (tratando-se do bloco do sistema de arquivos) os dados devem ser armazenados. Essa decisão é atrasada até o último momento possível. Alguns dados temporários de vida curta talvez nunca cheguem no disco, pois podem ficar obsoletos devido ao tempo que o XFS leva para decidir onde gravá-los. Portanto, o XFS aumenta o desempenho de gravação e reduz a fragmentação do sistema de arquivos. Como a alocação atrasada resulta em eventos de gravação menos freqüentes do que em outros sistemas de arquivos, é provável que a perda de dados depois de uma falha durante a gravação seja mais severa.

Pré-alocação para evitar a fragmentação do sistema de arquivos
Antes de gravar os dados no sistema de arquivos, o XFS *reserva* (pré-aloca) o espaço livre necessário para um arquivo. Portanto, a fragmentação do sistema de arquivos é amplamente reduzida. O desempenho aumenta porque o conteúdo dos arquivos não é distribuído em todo o sistema de arquivos.

34.3 Outros sistemas de arquivos suportados

Tabela 34.1, “Tipos de sistema de arquivos no Linux” (p 540) resume alguns dos sistemas de arquivos suportados pelo Linux. Eles são suportados principalmente para garantir a compatibilidade e o intercâmbio de dados com diferentes tipos de mídia de sistemas operacionais estrangeiros.

Tabela 34.1 *Tipos de sistema de arquivos no Linux*

`cramfs`	*Sistema de arquivos ROM compactado*: um sistema de arquivos compactados apenas leitura para ROMs.
`hpfs`	*Sistema de arquivos de alto desempenho*: o sistema de arquivos padrão da IBM OS/2 — suportado no modo apenas leitura.
`iso9660`	Sistema de arquivos padrão em CD-ROMs.
`minix`	Este sistema de arquivos foi originado de projetos acadêmicos em sistemas operacionais e foi o primeiro usado no Linux. Atualmente, ele é usado como um sistema de arquivos para disquetes.
`msdos`	*fat*, o sistema de arquivos originariamente usado por DOS, hoje é usado por vários sistemas operacionais.
`ncpfs`	Sistema de arquivos para montagem de volumes Novell em redes.
`nfs`	*Sistema de arquivos de rede*: os dados podem ser armazenados em qualquer máquina em uma rede, e o acesso pode ser concedido via rede.
`smbfs`	O *Bloco de Mensagens do Servidor* é usado por produtos como o Windows para permitir o acesso a arquivos em uma rede.
`sysv`	Usado no SCO UNIX, no Xenix e no Coherent (sistemas UNIX comerciais para PCs).
`ufs`	Usado por BSD, SunOS e NeXTstep. Suportado somente no modo apenas leitura.
`umsdos`	*UNIX em MS-DOS*: aplicado sobre um sistema de arquivos `fat` normal, atinge a funcionalidade UNIX (permissões, links, nomes longos de arquivos) criando arquivos especiais.
`vfat`	*Virtual FAT*: extensão do sistema de arquivos `fat` (suporta nomes longos de arquivos).

34.4 LFS (Large File Support - Suporte a Arquivos Grandes) no Linux

Originariamente, o Linux suportava um tamanho máximo de arquivo de 2 GB. Isso era o suficiente antes da explosão da multimídia e enquanto ninguém tentava manipular enormes bancos de dados no Linux. Ao se tornarem cada vez mais importantes na computação de servidores, o kernel e a biblioteca C foram modificados para suportar tamanhos de arquivo maiores que 2 GB, usados em um novo conjunto de interfaces que os aplicativos devem usar. Atualmente, todos os grandes sistemas de arquivos oferecem suporte a LFS, permitindo o desempenho de uma computação de ponta. A Tabela 34.2, “Tamanhos máximos de sistemas de arquivos (formato no disco)” (p 541) oferece uma visão geral das limitações atuais dos arquivos Linux e dos sistemas de arquivos.

Tabela 34.2 *Tamanhos máximos de sistemas de arquivos (formato no disco)*

Sistema de arquivos	Tamanho do arquivo (bytes)	Tamanho do sistema de arquivos (bytes)
Ext2 ou Ext3 (tamanho do bloco de 1 kB)	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 ou Ext3 (tamanho do bloco de 2 kB)	2^{38} (256 GB)	2^{43} (8 TB)
Ext2 ou Ext3 (tamanho do bloco de 4 kB)	2^{41} (2 TB)	2^{44} (16 TB)
Ext2 ou Ext3 (tamanho do bloco de 8 kB) (sistemas com páginas de 8 kB, como o Alpha)	2^{46} (64 TB)	2^{45} (32 TB)

Sistema de arquivos	Tamanho do arquivo (bytes)	Tamanho do sistema de arquivos (bytes)
ReiserFS v3	2^{46} (64 GB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
JFS (tamanho do bloco de 512 bytes)	2^{63} (8 EB)	2^{49} (512 TB)
JFS (tamanho do bloco de 4 kB)	2^{63} (8 EB)	2^{52} (4 PB)
NFSv2 (lado cliente)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (lado cliente)	2^{63} (8 EB)	2^{63} (8 EB)

IMPORTANTE: Limites de kernel do Linux

A Tabela 34.2, “Tamanhos máximos de sistemas de arquivos (formato no disco)” (p 541) descreve as limitações com relação ao formato no disco. O kernel 2.6 impõe seus próprios limites ao tamanho dos arquivos e aos sistemas de arquivos gerenciados por ele. Os limites são os seguintes:

Tamanho do arquivo
Em sistemas de 32 bits, os arquivos não podem exceder o tamanho de 2 TB (2^{41} bytes).

Tamanho do sistema de arquivos
Os sistemas de arquivos podem ter até 2^{73} de tamanho. Entretanto, esse limite ainda está fora do alcance para o hardware disponível atualmente.

34.5 Para obter mais informações

Cada projeto de sistema de arquivos descrito anteriormente mantém sua própria home page, na qual é possível encontrar informações de listas de discussão, outras documentações e FAQs (perguntas freqüentes).

- http://e2fsprogs.sourceforge.net/
- http://www.zipworld.com.au/~akpm/linux/ext3/
- http://www.namesys.com/
- http://oss.software.ibm.com/developerworks/opensource/jfs/
- http://oss.sgi.com/projects/xfs/

Um tutorial abrangente e multiparte sobre os sistemas de arquivos Linux pode ser encontrado em *IBM developerWorks*: http://www-106.ibm.com/developerworks/library/l-fs.html. Para obter uma comparação dos diferentes sistemas de arquivos de registro em diário no Linux, consulte o artigo de Juan I. Santos Florido em *Linuxgazette*: http://www.linuxgazette.com/issue55/florido.html. Os interessados em uma análise mais aprofundada do LFS no Linux podem acessar o site de Andreas Jaeger: http://www.suse.de/~aj/linux_lfs.html.

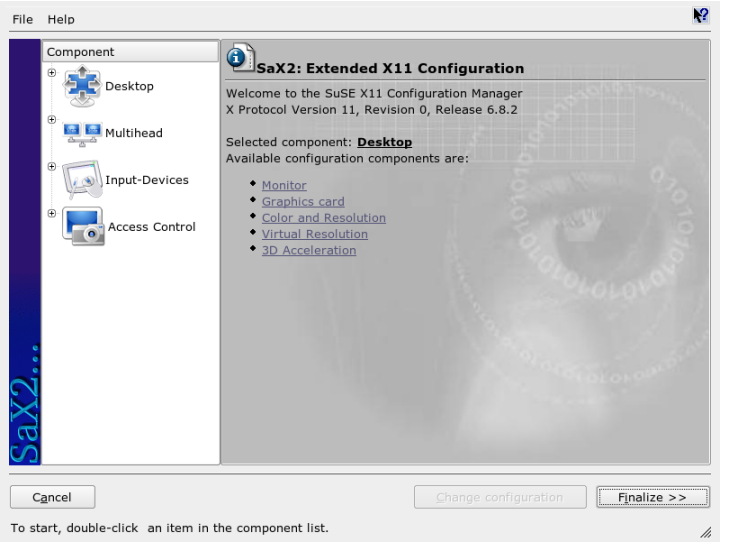
35 O sistema X Window

O sistema X Window (X11) é o padrão de fato para interfaces gráficas de usuário no UNIX. O X é baseado em rede, permitindo que aplicativos iniciados em um host sejam exibidos em outro host conectado em qualquer tipo de rede (LAN ou Internet). Este capítulo descreve a configuração e a otimização do ambiente do sistema X Window, fornece informações de base sobre o uso de fontes no SUSE Linux e explica a configuração do OpenGL e 3D.

35.1 Configuração do X11 com o SaX2

A interface gráfica de usuário, ou servidor X, lida com a comunicação entre o hardware e o software. Áreas de trabalho, como KDE e GNOME e a grande variedade de gerenciadores de janelas, usam o servidor X para interação com o usuário. A interface gráfica do usuário é inicialmente configurada durante a instalação. Para mudar depois as configurações, use o módulo respectivo do centro de controle do YaST ou execute o SaX2 manualmente da linha de comando com o comando `sax2`. A janela principal do SaX2 fornece um guarda-sol comum para os módulos individuais do centro de controle do YaST.

Figura 35.1 *A janela principal do SaX2*



Na barra de navegação esquerda, há seis itens, cada um mostrando a caixa de diálogo de configuração respectiva do centro de controle do YaST. Encontre as seções mencionadas abaixo no Chapter *Configuração do sistema com YaST* (↑Inicialização).

Monitor

Para obter uma descrição da configuração da placa de vídeo e o monitor, consulte a Seção “Propriedades da Placa e do Monitor” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

Mouse

Para obter uma descrição da configuração do mouse no ambiente gráfico, consulte a Seção “Propriedades do Mouse” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

Teclado

Para obter uma descrição da configuração do teclado no ambiente gráfico, consulte a Seção “Propriedades do Teclado” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

Mesa
Para obter uma descrição da configuração da mesa gráfica, consulte a Seção “Propriedades da mesa digitalizadora” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

Tela sensível ao toque
Para obter uma descrição da configuração da tela sensível ao toque, consulte a Seção “Propriedades da Tela Sensível ao Toque” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

VNC
Para obter uma descrição da configuração de VNC, consulte a Seção “Propriedades do Acesso Remoto” (Capítulo 3, *Configuração do sistema com YaST*, ↑Inicialização).

35.2 Otimizando a configuração do X

O X.Org é uma implementação de código-fonte aberto do sistema X Window. Ele também é desenvolvido pela X.Org Foundation, que é responsável ainda pelo desenvolvimento de novas tecnologias e padrões do sistema X Window.

Para usar da melhor forma possível o hardware disponível, inclusive o mouse, a placa gráfica, o monitor e o teclado, a configuração pode ser otimizada manualmente. Alguns aspectos desta otimização são explicados abaixo. Para obter informações detalhadas sobre como configurar o sistema X Window, consulte os vários arquivos no diretório `/usr/share/doc/packages/Xorg` e `man xorg.conf`.

ATENÇÃO

Tenha cuidado ao configurar o sistema X Window. Nunca inicie o sistema X Window antes que a configuração esteja concluída. Um sistema configurado de forma errada pode causar danos irreparáveis ao seu hardware (isso aplica-se especialmente a monitores de freqüência fixa). Os autores deste livro e o SUSE Linux não podem ser considerados responsáveis por danos. Essas informações foram pesquisadas cuidadosamente, mas isso não garante que todos os métodos apresentados aqui estejam corretos e não danifiquem o seu hardware.

Os programas SaX2 e xorgconfig criam o arquivo `xorg.conf`, por padrão no `/etc/X11`. Esse é o arquivo de configuração principal para o sistema X Window. A seguir estão todas as configurações referentes ao monitor, ao mouse e à placa de vídeo.

Os parágrafos a seguir descrevem a estrutura do arquivo de configuração `/etc/X11/xorg.conf`. Ela consiste em várias seções, cada uma delas referente a um determinado aspecto da configuração. Cada seção se inicia com a palavra-chave `Section <designation>` e termina com `EndSection`. As seções têm o seguinte formato:

```
Section designation
entry 1
entry 2
entry n
EndSection
```

Os tipos de seção disponíveis estão listados na Tabela 35.1, "Seções em /etc/X11/xorg.conf" (p 548).

Tabela 35.1 *Seções em /etc/X11/xorg.conf*

Tipo	Significado
`Files`	Esta seção descreve os caminhos usados por fontes e a tabela de cores RGB.
`ServerFlags`	Switches gerais são definidos aqui.
`InputDevice`	Dispositivos de entrada, como teclados e dispositivos de entrada especiais (touchpads, joysticks, etc.), são configurados nesta seção. Parâmetros importantes nesta seção são `Driver` e as opções que definem o `Protocol` e o `Device`.
`Monitor`	Descreve o monitor usado. Os elementos individuais desta seção são o nome, que é referenciado posteriormente na definição de `Screen`, a `bandwidth` e os limites de freqüência de sincronização (`HorizSync` e `VertRefresh`). As configurações são fornecidas em MHz, kHz e Hz. Normalmente, o servidor recusa qualquer linha modelo que não corresponda à especificação do monitor. Isso evita que freqüências muito altas sejam enviadas ao monitor por acidente.

Tipo	Significado
`Modes`	Os parâmetros da linha modelo são armazenados aqui para resoluções de tela específicas. Esses parâmetros podem ser calculados por SaX2 com base nos valores fornecidos pelo usuário e, normalmente, não precisam ser modificados. Intervenha manualmente neste ponto se, por exemplo, você desejar conectar um monitor de freqüência fixa. Há detalhes sobre o significado de valores numéricos individuais no arquivo HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
`Device`	Esta seção define uma placa de vídeo específica. Ela é referenciada por seu nome descritivo.
`Screen`	Esta seção junta um `Monitor` e um `Device` para formar todas as configurações necessárias para X.Org. Na subseção `Display`, especifique o tamanho da tela virtual (`Virtual`), a `ViewPort` e os `Modes` usados com esta tela.
`ServerLayout`	Esta seção define o layout de uma configuração única ou multihead. Esta seção junta os dispositivos de entrada `InputDevice` e os dispositivos de exibição `Screen`.

`Monitor`, `Device` e `Screen` são explicados em mais detalhes abaixo. Mais informações sobre as outras seções podem ser encontradas nas páginas de manual de `X.Org` e `xorg.conf`.

Há várias seções `Monitor` e `Device` diferentes em `xorg.conf`. Mesmo várias seções `Screen` são possíveis. A seção `ServerLayout` a seguir determina qual é usada.

35.2.1 Seção de Tela

Primeiro, observe atentamente a seção de tela, que combina um monitor com uma seção de dispositivo e determina a resolução e a intensidade de cor a serem usadas. Uma seção de tela pode ter a aparência do Exemplo 35.1, “Seção de tela do arquivo /etc/X11/xorg.conf” (p 550).

Exemplo 35.1 *Seção de tela do arquivo /etc/X11/xorg.conf*

```
Section "Screen"
DefaultDepth  16
SubSection "Display"
Depth       16
Modes       "1152x864" "1024x768" "800x600"
Virtual     1152x864
EndSubSection
SubSection "Display"
Depth       24
Modes       "1280x1024"
EndSubSection
SubSection "Display"
Depth       32
Modes "640x480"
EndSubSection
SubSection "Display"
Depth        8
Modes       "1280x1024"
EndSubSection
Device        "Device[0]"
Identifier    "Screen[0]"
Monitor       "Monitor[0]"
EndSection
```

A linha `Identifier` (aqui `Screen[0]`) fornece a esta seção um nome definido com o qual pode ser exclusivamente referenciado na seguinte seção `ServerLayout`. As linhas `Device` e `Monitor` especificam a placa de vídeo e o monitor que pertence a esta definição. Estes são links às seções `Device` e `Monitor` com seus nomes correspondentes ou *identificadores*. Estas seções são abordadas em detalhes abaixo.

Use a configuração `DefaultDepth` para selecionar a intensidade de cor que o servidor deve usar a menos que seja iniciado com uma intensidade de cor específica. Há uma subseção `Display` para cada intensidade de cor. A palavra-chave `Depth` atribui a intensidade de cor válida para essa subseção. Valores possíveis para `Depth` são 8, 15, 16 e 24. Nem todos os módulos do servidor X suportam esses valores.

Após a intensidade de cor, uma lista de resoluções é definida na seção `Modes`. O servidor X verifica essa lista da esquerda para a direita. Para cada resolução, o servidor X procura uma `Modeline` adequada na seção `Modes`. A `Modeline` depende da capacidade do monitor e da placa de vídeo. As configurações de `Monitor` determinam a `Modeline` resultante.

A primeira resolução encontrada é o `Default mode`. Com Ctrl + Alt + + (no teclado numérico), alterne para a resolução seguinte na lista à direita. Com Ctrl + Alt + – (no

teclado numérico), alterne para a esquerda. Isso permite a você variar a resolução enquanto o X está sendo executado.

A última linha da subseção `Display` com `Depth 16` refere-se ao tamanho da tela virtual. O tamanho máximo possível de uma tela virtual depende da quantidade de memória instalada na placa de vídeo e a intensidade de cor desejada, não a resolução máxima do monitor. Como placas de vídeo modernas têm uma grande quantidade de memória de vídeo, você pode criar áreas de trabalho virtuais bem grandes. Porém, você talvez não seja mais capaz de usar a funcionalidade de 3D se preencher a maior parte da memória de vídeo com uma área de trabalho virtual. Se a placa tem 16 MB de memória RAM de vídeo, por exemplo, a tela virtual pode ser de até 4096x4096 pixels em tamanho com intensidade de cor de 8 bits. Porém, principalmente para placas aceleradas, não é recomendável usar toda a memória para a tela virtual, pois a memória na placa também é usada para vários caches de vídeo e fontes.

35.2.2 Seção do dispositivo

Uma seção de dispositivo descreve uma placa de vídeo específica. Você pode ter quantas entradas de dispositivo em `xorg.conf` desejar, desde que os nomes sejam diferenciados, usando a palavra-chave `Identifier`. Como regra — se você tiver mais de uma placa de vídeo instalada — as seções são simplesmente numeradas em ordem. A primeira é chamada `Device[0]`, a segunda `Device[1]` e assim por diante. O arquivo a seguir mostra um exemplo da seção `Device` de um computador com uma placa de vídeo de PCI Matrox Millennium:

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Se você usar SaX2 para a configuração, a seção de dispositivo deve ter a aparência similar ao exemplo acima. Ambos o `Driver` e o `BusID` são dependentes do hardware instalado no seu computador e são detectados pelo SaX2 automaticamente. O `BusID` define o slot PCI ou AGP no qual a placa de vídeo está instalada. Isso corresponde ao ID exibido pelo comando lspci. O servidor X precisa de detalhes no formato decimal, mas o lspci os exibe no formato hexadecimal.

Através do parâmetro `Driver`, especifique o driver a ser usado para esta placa de vídeo. Se a placa for Matrox Millennium, o módulo do driver será chamado `mga`. Em seguida, o servidor X pesquisa através do `ModulePath` definido na seção `Files` no subdiretório `drivers`. Em uma instalação padrão, este é o diretório `/usr/X11R6/lib/modules/drivers`. `_drv.o` será adicionado ao nome, por isso, no caso do driver `mga`, o arquivo de driver `mga_drv.o` será carregado.

O comportamento do servidor X ou do driver também pode ser influenciado através de opções adicionais. Um exemplo disso é a opção `sw_cursor`, definida na seção de dispositivo. Isso desativa o cursor do mouse do hardware e mostra o cursor do mouse usando o software. Dependendo do módulo do driver, há várias opções disponíveis, que podem ser encontradas nos arquivos de descrição dos módulos do driver no diretório `/usr/X11R6/lib/X11/doc`. Geralmente, opções válidas também podem ser encontradas nas páginas de manual (`man xorg.conf` e `man X.Org`).

35.2.3 Seção Monitor e Modos

Como as seções `Device`, as seções `Monitor` e `Modes` descrevem um monitor cada. O arquivo de configuração `/etc/X11/xorg.conf` pode conter quantas seções `Monitor` você desejar. A seção de layout do servidor especifica qual seção `Monitor` é relevante.

Definições de monitor devem ser configuradas por usuários experientes. As linhas modelo constituem uma parte importante das seções `Monitor`. Linhas modelo definem temporizações verticais para a respectiva resolução. As propriedades do monitor, especialmente as freqüências permitidas, estão armazenadas na seção `Monitor`.

ATENÇÃO

A menos que você tenha um conhecimento profundo de funções de monitor e placa de vídeo, nada deve ser mudado nas linhas modelo, pois isso poderia causar danos severos ao seu monitor.

As pessoas que tentam desenvolver suas próprias descrições de monitor devem estar familiarizadas com a documentação em `/usr/X11/lib/X11/doc`. A seção cobrindo os modos de vídeo merece uma atenção especial. Ela descreve, em detalhes, como o hardware funciona e como criar linhas modelo.

A especificação manual de linhas modelo raramente é exigida atualmente. Se você está usando um monitor multisync moderno, as freqüências permitidas e as resoluções ótimas podem, como regra, serem lidas do monitor pelo servidor X através de DDC, como descrito na seção de configuração do SaX2. Se isso não for possível por algum motivo, use um dos modos VESA incluídos no servidor X. Isso funcionará com praticamente todas as combinações de monitor e placa de vídeo.

35.3 Instalando e configurando fontes

A instalação de fontes adicionais no SUSE Linux é muito fácil. Simplesmente copie as fontes para qualquer diretório localizado no caminho da fonte X11 (consulte a Seção 35.3.2, “Fontes centrais X11” (p 557)). Para habilitar o uso das fontes, o diretório de instalação deve ser um subdiretório dos diretórios configurados em `/etc/fonts/fonts.conf` (consulte a Seção 35.3.1, “Xft” (p 554)).

Os arquivos de fontes podem ser copiados manualmente (como `root`) para um diretório adequado, como `/usr/X11R6/lib/X11/fonts/truetype`. Alternativamente, a tarefa pode ser realizada com o instalador de fontes do KDE no Centro de Controle do KDE. O resultado é o mesmo.

Em vez de copiar as fontes reais, você também pode criar links simbólicos. Por exemplo, é recomendável fazer isso se você tem fontes licenciadas em uma partição do Windows montada e deseja usá-las. Em seguida, execute `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` executa o script `/usr/sbin/fonts-config`, que lida com a configuração das fontes. Para ver o que o script faz, consulte a página de manual do script (`man fonts-config`).

O procedimento é o mesmo para fontes de bitmap, fontes TrueType e OpenType e fontes Type1 (PostScript). Todos esses tipos de fonte podem ser instalados em qualquer diretório. Somente fontes indexadas ao CID exigem um procedimento um pouco diferente. Para isso, consulte a Seção 35.3.3, “Fontes indexadas do CID” (p 558).

X.Org contém dois sistemas de fontes completamente diferentes: O *sistema de fontes central X11* antigo e o sistema *Xft and fontconfig* recém-criado. As seções a seguir descrevem brevemente esses dois sistemas.

35.3.1 Xft

Desde o início, os programadores do Xft certificaram-se de que as fontes escaláveis, incluindo as de antialiasing, tivessem suporte adequado. Se o Xft for usado, as fontes serão exibidas pelo aplicativo usando as fontes, não pelo servidor X como no sistema de fontes central X11. Desta forma, o respectivo aplicativo tem acesso aos arquivos de fontes reais e controle total sobre como os glifos são exibidos. Isso constitui a base para a exibição correta do texto em vários idiomas. Acesso direto aos arquivos de fontes é bastante útil para embutir fontes para impressão para certificar-se de que a impressão tem a mesma aparência da saída da tela.

No SUSE Linux, os dois ambientes de área de trabalho do KDE e do GNOME, Mozilla, e vários outros aplicativos já usam o Xft por padrão. O Xft já é usado por mais aplicativos do que o sistema de fontes central X11 antigo.

O Xft usa a biblioteca fontconfig para localizar fontes e influenciar como elas são exibidas. As propriedades de fontconfig são controladas pelo arquivo de configuração global `/etc/fonts/fonts.conf` e o arquivo de configuração específico ao usuário `~/.fonts.conf`. Cada um destes arquivos de configuração fontconfig deve iniciar com

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

e terminar com

```
</fontconfig>
```

Para adicionar diretórios para pesquisar fontes, acrescente linhas como as seguintes:

```
<dir>/usr/local/share/fonts/</dir>
```

Porém, isso geralmente não é necessário. Por padrão, o diretório específico ao usuário `~/.fonts` já está inserido em `/etc/fonts/fonts.conf`. Da mesma maneira, tudo o que você precisa fazer para instalar fontes adicionais é copiá-las para `~/.fonts`.

Você também pode inserir regras que influenciam a aparência das fontes. Por exemplo, digite

```
<match target="font">
<edit name="antialias" mode="assign">
<bool>false</bool>
```

```
</edit>
</match>
```

Para desabilitar o antialiasing para todas as fontes ou

```
<match target="font">
<test name="family">
<string>Luxi Mono</string>
<string>Luxi Sans</string>
</test>
<edit name="antialias" mode="assign">
<bool>false</bool>
</edit>
</match>
```

para desabilitar o antialiasing para fontes específicas.

Por padrão, a maioria dos aplicativos usa os nomes de fontes `sans-serif` (ou o equivalente `sans`), `serif` ou `monospace`. Estas não são fontes reais, mas somente aliás que são resolvidos para uma fonte adequada, dependendo da configuração de idioma.

Usuários podem facilmente adicionar regras para `~/.fonts.conf` a fim de resolver esses aliás para suas fontes favoritas:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Como quase todos os aplicativos usam esses aliás por padrão, isso afeta praticamente todo o sistema. Desta forma, você pode facilmente usar suas fontes favoritas praticamente em qualquer local sem precisar modificar as configurações de fontes nos aplicativos individuais.

Use o comando `fc-list` para encontrar as fontes instaladas e disponíveis para uso. Por exemplo, o comando `fc-list` retorna uma lista de todas as fontes. Para descobrir quais das fontes escaláveis disponíveis (`:outline=true`) contêm todos os glifos exigidos para hebraico (`:lang=he`), os nomes de fontes (`family`), o estilo (`style`), o peso (`weight`) e o nome dos arquivos contendo as fontes, digite o seguinte comando:

```
fc-list ":lang=he:outline=true" family style weight
```

A saída do comando pode ter a seguinte aparência:

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Parâmetros importantes podem ser consultados com `fc-list`:

Tabela 35.2 *Parâmetros de fc-list*

Parâmetro	Significado e valores possíveis
`family`	Nome da família da fonte, por exemplo, `FreeSans`.
`foundry`	Nome do fabricante da fonte, por exemplo, `urw`.
`style`	O estilo da fonte, como `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`.
`lang`	O idioma que a fonte suporta, por exemplo, `de` para alemão, `ja` para japonês, `zh-TW` para chinês tradicional ou `zh-CN` para chinês simplificado.
`weight`	O peso da fonte, como `80` para normal, `200` para negrito.
`slant`	A inclinação, geralmente `0` para nenhum e `100` para itálico.

Parâmetro	Significado e valores possíveis
`file`	O nome do arquivo contendo a fonte.
`outline`	`true` para fontes de bordas, `false` para outras fontes.
`scalable`	`true` para fontes escaláveis, `false` para outras fontes.
`bitmap`	`true` para fontes de bitmap, `false` para outras fontes.
`pixelsize`	Tamanho de fonte em pixels. Em conexão com a fc-list, esta opção só faz sentido para fontes de bitmap.

35.3.2 Fontes centrais X11

Atualmente, o sistema de fontes centrais X11 suporta não somente fontes de bitmap, mas também fontes escaláveis, como fontes Type1, TrueType e OpenType e fontes indexadas do CID. Fontes Unicode também já têm suporte há algum tempo. Em 1987, o sistema de fontes centrais X11 foi desenvolvido originalmente para X11R1 para o propósito de processar fontes de bitmap monocromáticas. Todas as extensões mencionadas acima foram adicionadas posteriormente.

Fontes escaláveis são suportadas somente sem a exibição de subpixel e antialiasing e o carregamento de fontes escaláveis grandes para vários idiomas pode levar muito tempo. O uso de fontes Unicode também pode ser lento e exige mais memória.

O sistema de fontes centrais X11 tem algumas fraquezas inerentes. Ele está desatualizado e não pode mais ser estendido de forma significativa. Embora ele possa ser mantido por motivos de compatibilidade retroativa, o sistema Xft e fontconfig mais moderno deve ser usado se for possível.

Para essa operação, o servidor X precisa saber quais fontes estão disponíveis e onde no sistema ele pode encontrá-las. Isso é tratado por uma variável FontPath, que contém o caminho para todos os diretórios de fontes de sistemas válidos. Em cada um desses diretórios, um arquivo chamado `fonts.dir` lista as fontes disponíveis neste diretório. O FontPath é gerado pelo servidor X na inicialização. Ele procura um arquivo `fonts.dir` válido em cada uma das entradas `FontPath` no arquivo de configuração `/etc/X11/xorg.conf`. Essas entradas são encontradas na seção `Files`. Exiba o FontPath

real com `xset q`. Esse caminho também pode ser modificado no tempo de execução com xset. Para adicionar um outro caminho, use `xset +fp <path>`. Para remover um caminho indesejado, use `xset -fp <path>`.

Se o servidor X já estiver ativo, fontes recém-instaladas em diretórios montados podem tornar-se disponíveis com o comando `xset fp rehash`. Este comando é executado por `SuSEconfig --module fonts`. Como o comando `xset` precisa de acesso ao servidor X em execução, isso funciona somente se `SuSEconfig --module fonts` for iniciado de um shell com acesso ao servidor X em execução. A maneira mais fácil de conseguir isso é assumir permissões de `root` digitando `su` e a senha de root. `su` transfere as permissões de acesso do usuário que iniciou o servidor X para o shell do root. Para verificar se as fontes foram instaladas corretamente e estão disponíveis através do sistema de fontes centrais X11, use o comando `xlsfonts` para listar todas as fontes disponíveis.

Por padrão, o SUSE Linux usa locales UTF-8. Desta forma, fontes Unicode devem ser preferidas (nomes de fontes terminando com `iso10646-1` na saída `xlsfonts`). Todas as fontes Unicode disponíveis podem ser listadas com `xlsfonts | grep iso10646-1`. Praticamente todas as fontes Unicode disponíveis no SUSE Linux contêm pelo menos os glifos necessários para idiomas europeus (anteriormente codificado como `iso-8859-*`).

35.3.3 Fontes indexadas do CID

Em contraste com outros tipos de fontes, você não pode simplesmente instalar fontes indexadas do CID em somente qualquer diretório. Fontes indexadas do CID devem ser instaladas em `/usr/share/ghostscript/Resource/CIDFont`. Isso não é relevante para Xft e fontconfig, mas é necessário para Ghostscript e o sistema de fontes centrais X11.

DICA

Consulte `http://www.xfree86.org/current/fonts.html` para obter mais informações sobre fontes sob X11.

35.4 Configuração 3D do OpenGL

35.4.1 Suporte a hardware

O SUSE Linux inclui vários drivers do OpenGL para suporte a hardware 3D. A Tabela 35.3, “Hardware 3D suportados” (p 559) fornece uma visão geral.

Tabela 35.3 *Hardware 3D suportados*

Driver do OpenGL	Hardware suportado
nVidia	nVidia Chips: todos, com exceção do Riva 128(ZX)
DRI	3Dfx Voodoo Banshee,
	3Dfx Voodoo-3/4/5,
	Intel i810/i815/i830M,
	Intel 845G/852GM/855GM/865G/915,
	Matrox G200/G400/G450/G550,
	ATI Rage 128(Pro)/Radeon (até 9250)

Se você estiver fazendo uma instalação com o YaST pela primeira vez, a aceleração 3D poderá ser ativada durante a instalação, uma vez que o YaST detecta suporte a 3D. Para chips de gráficos nVidia, é necessário instalar o driver nVidia antes. Para fazer isso, selecione o patch do driver nVidia em YOU (YaST Online Update - Atualização Online do YaST). Devido a restrições de licença, o driver do nVidia não está incluído na distribuição.

O procedimento de configuração do suporte ao hardware 3D será diferente, caso uma atualização esteja sendo usada, em vez de uma nova instalação, ou caso seja necessário configurar um adaptador gráfico de expansão 3Dfx (Voodoo Graphics ou Voodoo-2). Isso depende de qual driver do OpenGL está sendo usado. Detalhes adicionais serão fornecidos na próxima seção.

35.4.2 Drivers do OpenGL

Os drivers nVidia e DRI do OpenGL podem ser facilmente configurados com SaX2. Para adaptadores nVidia, é necessário instalar o driver nVidia antes. Digite o comando `3Ddiag` para verificar se a configuração do nVidia ou DRI está correta.

Por razões de segurança, somente usuários pertencentes ao grupo `vídeo` têm permissão para acessar o hardware 3D. Portanto, verifique se todos os usuários locais são membros desse grupo. Caso contrário, o *fallback de renderização de software* lento do driver do OpenGL será usado para aplicativos do OpenGL. Use o comando `id` para verificar se o usuário atual pertence ao grupo `vídeo`. Se não for o caso, use o YaST para adicionar o usuário ao grupo.

35.4.3 Ferramenta de diagnóstico 3Ddiag

A ferramenta de diagnóstico 3Ddiag permite verificar a configuração 3D do SUSE Linux. Essa é uma ferramenta da linha de comando que deve ser iniciada em um terminal. Digite `3Ddiag -h` para relacionar possíveis opções para a 3Ddiag.

Para verificar a configuração de X.Org, a ferramenta verifica se os pacotes necessários para o suporte 3D estão instalados e se a biblioteca do OpenGL e a extensão GLX corretas estão sendo usadas. Se receber mensagens de falha, siga as instruções da 3Ddiag. Se tudo estiver correto, serão exibidas somente mensagens de conclusão na tela.

35.4.4 Utilitários de teste do OpenGL

Para testar o OpenGL, pode ser útil usar o programa `glxgears` e jogos como `tuxracer` e `armagetron` (os pacotes têm os mesmos nomes). Se o suporte 3D tiver sido ativado, será possível reproduzi-los adequadamente em um computador novo. Sem suporte 3D, esses jogos seriam executados muito lentamente (efeito apresentação de slide). Use o comando `glxinfo` para verificar se o 3D está ativo. Em caso positivo, a saída conterá uma linha com `direct rendering: Yes`.

35.4.5 Solucionando problemas

Se os resultados do teste 3D do OpenGL forem negativos (os jogos não forem reproduzidos adequadamente), use a 3Ddiag para verificar se não há erros na configuração (mensagens de erro). Se a correção não ajudar ou as mensagens de erro não tiverem sido exibidas, analise os arquivos de registro X.Org.

Com freqüência, você encontrará a linha `DRI is disabled` no arquivo X.Org `/var/log/Xorg.0.log`. A causa exata só poderá ser descoberta por meio de um exame detalhado do arquivo de registro, tarefa que requer experiência.

Em tais casos, não há erros de configuração, pois eles teriam sido detectados pela 3Ddiag. Conseqüentemente, nesse ponto a única alternativa é usar o fallback de renderização do software do driver DRI, que não fornece suporte a hardware 3D. Você também deverá ficar sem suporte a 3D, se houver instabilidade ou erros de representação do OpenGL. Use o SaX2 para desabilitar totalmente o suporte a 3D.

35.4.6 Suporte à instalação

Além do `fallback de renderizaç o de software` do driver DRI, todos os drivers do OpenGL no Linux estão em fase de desenvolvimento e, portanto, são considerados experimentais. Os drivers são incluídos na distribuição devido à alta demanda de aceleração do hardware 3D no Linux. Considerando o status experimental dos drivers do OpenGL, o SUSE não pode oferecer suporte à instalação para configuração da aceleração do hardware 3D, nem fornecer assistência adicional a problemas relacionados. A configuração básica da interface gráfica do usuário (sistema X Window) não inclui configuração de aceleração do hardware 3D. Se você tiver problemas com a aceleração do hardware 3D, é recomendável desabilitar totalmente o suporte a 3D.

35.4.7 Documentação online adicional

Para obter informações sobre DRI, consulte `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`) Mais informações sobre a instalação do driver nvidia são encontradas em http://ftp.suse.com/pub/suse/i386/supplementary/X/nvidia-installer-HOWTO.html.

36 Autenticação com o PAM

O Linux usa o PAM (Pluggable Authentication Modules) no processo de autenticação como uma camada mediadora entre o usuário e o aplicativo. Como os módulos PAM estão disponíveis em todo o sistema, eles podem ser solicitados por qualquer aplicativo. Este capítulo descreve o funcionamento e a configuração do mecanismo de autenticação modular.

Os programadores e administradores do sistema muitas vezes desejam restringir o acesso a certas partes do sistema ou limitar o uso de certas funções de um aplicativo. Sem o PAM, os aplicativos precisam ser adaptados toda vez que é introduzido um novo mecanismo de autenticação, como o LDAP ou o SAMBA. Entretanto, esse processo é bastante demorado e propenso a erros. Uma forma de evitar essas desvantagens é separar os aplicativos do mecanismo de autenticação e delegar este último a módulos gerenciados centralmente. Sempre que um esquema de autenticação passa a ser necessário, basta adaptar ou gravar um módulo PAM adequado para ser usado pelo programa em questão.

Todo programa baseado no mecanismo PAM tem um arquivo de configuração próprio no diretório `/etc/pam.d/`*`programname`*. Esses arquivos definem os módulos PAM usados para a autenticação. Além disso, existem arquivos de configuração globais para a maioria dos módulos PAM em `/etc/security`, que definem o exato comportamento desses módulos (alguns exemplos são `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf` e `time.conf`). Todo aplicativo que usa um módulo PAM na realidade chama um conjunto de funções do PAM que, em seguida, processa as informações nos diversos arquivos de configuração e apresenta o resultado ao aplicativo que chamou.

36.1 Estrutura de um arquivo de configuração PAM

Cada linha de um arquivo de configuração PAM contém, no máximo, quatro colunas:

```
<Tipo de módulo> <Flag de controle> <Caminho do módulo> <Opções>
```

Os módulos PAM são processados como pilhas. Diferentes tipos de módulos servem a diferentes objetivos. Por exemplo, um módulo verifica a senha, outro verifica a localização de onde o sistema está sendo acessado e outro lê configurações específicas ao usuário. O PAM tem conhecimento sobre quatro tipos diferentes de módulos:

`auth (autenticação)`
: O objetivo desse tipo de módulo é verificar a autenticidade do usuário. Essa verificação tradicionalmente é feita por meio de uma consulta a senha, mas também pode ser realizada com a ajuda de um cartão com chip ou de biometria (impressões digitais ou leitura da íris).

`account (conta)`
: Os módulos desse tipo verificam se o usuário possui uma permissão geral para usar o serviço solicitado. A título de exemplo, essa verificação deve ser realizada para assegurar que ninguém seja capaz de efetuar o login com o nome de usuário de uma conta vencida.

`password (senha)`
: O objetivo desse tipo de módulo é permitir a mudança de um token de autenticação. Na maioria dos casos, trata-se de uma senha.

`session (sessão)`
: Os módulos desse tipo são responsáveis pelo gerenciamento e configuração de sessões de usuários. Eles são iniciados antes e depois da autenticação para registrar tentativas de login em registros do sistema e para configurar o ambiente específico do usuário (contas de e-mail, diretório pessoal, limites do sistema etc.).

A segunda coluna contém flags de controle para influenciar o comportamento dos módulos iniciados:

required (obrigatório)
Um módulo com esse flag precisa ser processado com êxito para que a autenticação possa prosseguir. Após a falha de um módulo com o flag `required` (obrigatório), todos os outros módulos com o mesmo flag serão processados antes que o usuário receba uma mensagem sobre a falha da tentativa de autenticação.

requisite (necessário)
Os módulos com esse flag também precisam ser processados com êxito, de modo bastante semelhante ao módulo com o flag `required` (obrigatório). Contudo, em caso de falha, um módulo com esse flag dá um retorno imediato ao usuário e os módulos restantes deixam de ser processados. Em caso de êxito, os outros módulos são processados, exatamente como qualquer módulo com o flag `required` (obrigatório). O flag `requisite` (necessário) pode ser usado como um filtro básico para verificar a existência de determinadas condições essenciais para a correta autenticação.

sufficient (suficiente)
Após o processamento com êxito de um módulo com esse flag, o aplicativo que chamou recebe imediatamente uma mensagem sobre o êxito e o processamento dos módulos é interrompido, exceto quando houver falhas anteriores em um módulo com o flag `required` (obrigatório). A falha de um módulo com o flag `sufficient` (suficiente) não traz conseqüências diretas, com os módulos subseqüentes sendo processados na sua respectiva ordem.

optional (opcional)
A falha ou êxito de um módulo com esse flag não traz conseqüências diretas. Isso pode ser útil no caso de módulos cujo único propósito é exibir uma mensagem (por exemplo, informar ao usuário sobre a chegada de e-mails) sem executar nenhuma ação adicional.

include (incluir)
Quando esse flag é dado, o arquivo especificado como argumento é inserido nesse lugar.

O caminho do módulo não precisa ser explicitado, contanto que o módulo fique localizado no diretório padrão `/lib/security` (para todas as plataformas de 64 bits suportadas pelo SUSE Linux, o diretório é `/lib64/security`). A quarta coluna pode conter uma opção para o módulo específico, como `debug` (permite a depuração) ou `nullok` (permite o uso de senhas vazias).

36.2 A configuração PAM do sshd

Para demonstrar o funcionamento da teoria do PAM, considere a configuração PAM do sshd como um exemplo prático:

Exemplo 36.1 *Configuração PAM do sshd*

```
#%PAM-1.0
auth     include        common
auth auth     required       pam_nologin.so
account  include        common-account
password include        common-password
session  include        common-session
# Habilitar a seguinte linha para obter suporte de resmgr para
# sessões ssh (consulte /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

A configuração PAM típica de um aplicativo (sshd, nesse caso) contém quatro instruções include (incluir) referentes aos arquivos de configuração de quatro tipos de módulo: `common-auth`, `common-account`, `common-password` e `common-session`. Esses quatro arquivos abrigam a configuração padrão de cada tipo de módulo. Ao incluí-los em vez de chamar cada módulo separadamente para cada aplicativo do PAM, será possível obter automaticamente uma configuração PAM atualizada se o administrador mudar os padrões. Antigamente, era necessário fazer o ajuste manual de todos os arquivos de configuração para todos os aplicativos quando ocorriam mudanças no PAM ou quando um novo aplicativo era instalado. Agora, a configuração PAM é feita com arquivos de configuração centrais e todas as mudanças são automaticamente herdadas pela configuração PAM de cada serviço.

O primeiro arquivo incluído (`common-auth`) chama dois módulos do tipo `auth` (autenticação): `pam_env` e `pam_unix2`. Consulte Exemplo 36.2, “Configuração padrão da seção `auth` (autenticação)” (p 566).

Exemplo 36.2 *Configuração padrão da seção auth (autenticação)*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

O primeiro, `pam_env`, carrega o arquivo `/etc/security/pam_env.conf` para definir as variáveis de ambiente conforme especificado nesse arquivo. Esse módulo pode ser usado para definir o valor correto da variável `DISPLAY`, pois o módulo `pam_env` tem conhecimento do local de onde o login está sendo feito. O segundo, `pam_unix2`, compara o login e a senha do usuário a `/etc/passwd` e `/etc/shadow`.

Depois da chamada com êxito dos módulos especificados em `common-auth`, um terceiro módulo chamado `pam_nologin` verifica se o arquivo `/etc/nologin` existe. Em caso afirmativo, somente o usuário `root` poderá efetuar o login. A pilha inteira de módulos `auth` (autenticação) é processada antes que o sshd receba qualquer retorno sobre o êxito do login. Tendo em vista que todos os módulos da pilha apresentam o flag de controle `required` (obrigatório), todos precisam ser processados com êxito antes que o sshd receba uma mensagem sobre o resultado positivo. Se algum dos módulos falhar, a pilha de módulos inteira ainda será processada e somente aí é que o sshd será notificado sobre o resultado negativo.

Logo após o processamento com êxito de todos os módulos do tipo `auth` (autenticação), outra instrução include (incluir) é processada. Nesse caso, a que está em Exemplo 36.3, "Configuração padrão da seção `account` (conta)" (p 567). O `common-account` contém apenas um módulo, o `pam_unix2`. Se o `pam_unix2` retornar o resultado de que o usuário existe, o sshd receberá uma mensagem de êxito e a próxima pilha de módulos (`password` - senha) será processada, conforme mostrado em Exemplo 36.4, "Configuração padrão da seção `password` (senha)" (p 567).

Exemplo 36.3 *Configuração padrão da seção account (conta)*

```
account required        pam_unix2.so
```

Exemplo 36.4 *Configuração padrão da seção password (senha)*

```
password required       pam_pwcheck.so  nullok
password required       pam_unix2.so    nullok use_first_pass use_authtok
#password required      pam_make.so     /var/yp
```

Mais uma vez, a configuração PAM do sshd envolve apenas uma instrução include (incluir) referente à configuração padrão dos módulos `password` (senha) localizados em `common-password`. Esses módulos precisam ser concluídos com êxito (flag de controle `required` - obrigatório) sempre que o aplicativo solicita a mudança de um token de autenticação. A mudança de uma senha ou de outro token de autenticação requer uma verificação de segurança. Essa ação é possibilitada pelo módulo `pam_pwcheck`. O módulo `pam_unix2` usado posteriormente vem com quaisquer senhas antigas e novas do módulo `pam_pwcheck`, de modo que o usuário não precise autenticar novamente. Isso também torna impossível driblar as verificações realizadas pelo `pam_pwcheck`. Os módulos do tipo `password` (senha) devem ser usados sempre que os módulos precedentes do tipo `account` (conta) ou `auth` (autenticação) são configurados para fazer uma queixa sobre uma senha vencida.

Exemplo 36.5 *Configuração padrão da seção session (sessão)*

```
session required        pam_limits.so
session required        pam_unix2.so
```

Na etapa final, os módulos do tipo `session` (sessão), integrados no arquivo `common-session`, são chamados para configurar a sessão de acordo com as configurações do usuário em questão. Embora o `pam_unix2` seja processado novamente, não há conseqüências práticas devido à opção `none` (nenhum) especificada no respectivo arquivo de configuração desse módulo, o `pam_unix2.conf`. O módulo `pam_limits` carrega o arquivo `/etc/security/limits.conf`, que pode definir limites sobre o uso de certos recursos do sistema. Os módulos `session` (sessão) são chamados uma segunda vez quando o usuário efetua logout.

36.3 Configuração de módulos PAM

Alguns dos módulos PAM são configuráveis. Os arquivos de configuração correspondentes estão localizados em `/etc/security`. Essa seção apresenta uma breve descrição dos arquivos de configuração relevantes para o exemplo do sshd: `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` e `limits.conf`.

36.3.1 pam_unix2.conf

O método tradicional de autenticação baseada em senha é controlado pelo módulo PAM `pam_unix2`. Ele consegue ler os dados necessários de `/etc/passwd`, `/etc/shadow`, mapas NIS, tabelas NIS+ ou de um banco de dados LDAP. Para influenciar o comportamento desse módulo, configure as opções de PAM do aplicativo em si ou efetue uma mudança global editando `/etc/security/pam_unix2.conf`. Um arquivo de configuração do módulo bastante básico é mostrado em Exemplo 36.6, “pam_unix2.conf” (p 568).

Exemplo 36.6 *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

A opção `nullok` para os tipos de módulo `auth` (autenticação) e `password` (senha) especifica que senhas vazias são permitidas para o tipo de conta correspondente. Os

usuários também têm permissão para mudar as senhas de suas contas. A opção `none` (nenhum) do tipo de módulo `session` (sessão) especifica que nenhuma mensagem foi registrada em seu nome (esse é o padrão). Obtenha mais informações sobre opções adicionais de configuração nos comentários do próprio arquivo e na página pam_unix2(8) do manual.

36.3.2 pam_env.conf

Esse arquivo pode ser usado para definir um ambiente padronizado para os usuários que será definido sempre que o módulo `pam_env` for chamado. Com ele, predefina variáveis de ambiente usando a seguinte sintaxe:

```
VARI VEL  [DEFAULT=[valor]]  [OVERRIDE=[valor]]
```

VARIÁVEL
Nome da variável de ambiente a ser definida.

[DEFAULT=[valor]]
Valor padrão que o administrador deseja definir.

[OVERRIDE=[valor]]
Os valores que podem ser usados para consulta e definidos por `pam_env`, substituindo o valor padrão.

Um exemplo típico de como o módulo `pam_env` pode ser usado é a adaptação da variável `DISPLAY`, que é mudada sempre que ocorre um login remoto. Você pode ver isso na Exemplo 36.7, “pam_env.conf” (p 569).

Exemplo 36.7 *pam_env.conf*

```
REMOTEHOST     DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY        DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

A primeira linha define o valor da variável `REMOTEHOST` para o `localhost`, que é usada sempre que `pam_env` não puder determinar qualquer outro valor. A variável `DISPLAY`, por sua vez, contém o valor de `REMOTEHOST`. Mais informações podem ser encontradas nos comentários do arquivo `/etc/security/pam_env.conf`.

36.3.3 pam_pwcheck.conf

Esse arquivo de configuração se destina ao módulo `pam_pwcheck`, que lê opções dele para todos os módulos do tipo `password` (senha). As configurações armazenadas nesse arquivo têm prioridade sobre as configurações PAM de um aplicativo individual. Se configurações específicas a um aplicativo não tiverem sido definidas, o aplicativo usará as configurações globais. Exemplo 36.8, “pam_pwcheck.conf” (p 570) instrui o módulo `pam_pwcheck` a permitir senhas vazias e a modificação de senhas. Mais opções para o módulo são citadas no arquivo `/etc/security/pam_pwcheck.conf`.

Exemplo 36.8 *pam_pwcheck.conf*

```
password:    nullok
```

36.3.4 limits.conf

Os limites do sistema podem ser definidos para um usuário ou para um grupo no arquivo `limits.conf`, que é lido pelo módulo `pam_limits`. O arquivo permite a definição de limites fixos, que não podem ser excedidos em hipótese alguma, e limites flexíveis, que podem ser excedidos temporariamente. Para obter informações sobre a sintaxe e as opções disponíveis, leia os comentários contidos no arquivo.

36.4 Mais informações

No diretório `/usr/share/doc/packages/pam` do sistema instalado, você encontra a seguinte documentação adicional:

READMEs
: No nível superior desse diretório, há alguns arquivos README gerais. O subdiretório `modules` abriga arquivos README sobre os módulos PAM disponíveis.

The Linux-PAM System Administrators' Guide (Guia do Administrador do Sistema Linux-PAM)
: Esse documento contém todas as informações que o administrador do sistema deve saber sobre o PAM. Ele aborda uma variedade de tópicos, desde a sintaxe dos

arquivos de configuração até os aspectos de segurança do PAM. O documento está disponível em formato PDF, HTML e como texto simples.

The Linux-PAM Module Writers' Manual (Manual do Elaborador de Módulos Linux-PAM)

Esse documento sintetiza esse tópico do ponto de vista do desenvolvedor, com informações sobre como elaborar módulos PAM em conformidade com os padrões. O documento está disponível em formato PDF, HTML e como texto simples.

The Linux-PAM Application Developers' Guide (Guia do Desenvolvedor de Aplicativos Linux-PAM)

Esse documento contém todas as informações necessárias a um desenvolvedor de aplicativos que queira usar as bibliotecas PAM. O documento está disponível em formato PDF, HTML e como texto simples.

Thorsten Kukuk desenvolveu uma série de módulos PAM para o SUSE Linux e disponibilizou algumas informações a esse respeito em `http://www.suse.de/~kukuk/pam/`.

37 Virtualização com o Xen

O Xen torna possível executar vários sistemas Linux em uma máquina física. O hardware para os sistemas diferentes é fornecido virtualmente. Este capítulo fornece uma visão geral das possibilidades e limitações desta tecnologia. As seções sobre instalação, configuração e execução do Xen completam essa introdução.

Máquinas virtuais comumente precisam emular o hardware que o sistema precisa. A desvantagem é que o hardware emulado é mais lento do que o silício real. O Xen tem uma abordagem diferente. Ele restringe a emulação para o mínimo de partes possível. Para obter isso, o Xen usa a *paravirtualização*. Esta é uma técnica que apresenta máquinas virtuais similarmente, mas não identicamente ao hardware subjacente. Portanto, os sistemas operacionais de host e convidados estão adaptados no nível do kernel. O espaço do usuário permanece inalterado. O Xen controla o hardware com um hypervisor e um convidado de controle, também chamado domain-0. Eles fornecem todos os dispositivos de rede e blocos virtualizados necessários. Os sistemas convidados usam esses dispositivos de rede e blocos virtuais para executar o sistema e conectar-se a outros convidados ou à rede local. Quando várias máquinas físicas executando o Xen são configuradas de forma que os dispositivos e rede e os blocos virtuais estejam disponíveis, também é possível migrar um sistema convidado de um equipamento de hardware para outro enquanto ele está em execução. Originalmente o Xen foi desenvolvido para executar até 100 sistemas convidados em um computador, mas esse número depende bastante dos requisitos de sistema dos sistemas convidados em execução, especialmente o consumo de memória.

Para limitar o uso de CPU, o hypervisor do Xen oferece três programadores diferentes. O programador também pode ser mudado durante a execução do sistema convidado, tornando possível mudar a prioridade da execução do sistema convidado. Em um nível

mais alto, migrar um convidado também pode ser usado para ajustar a energia do CPU disponível.

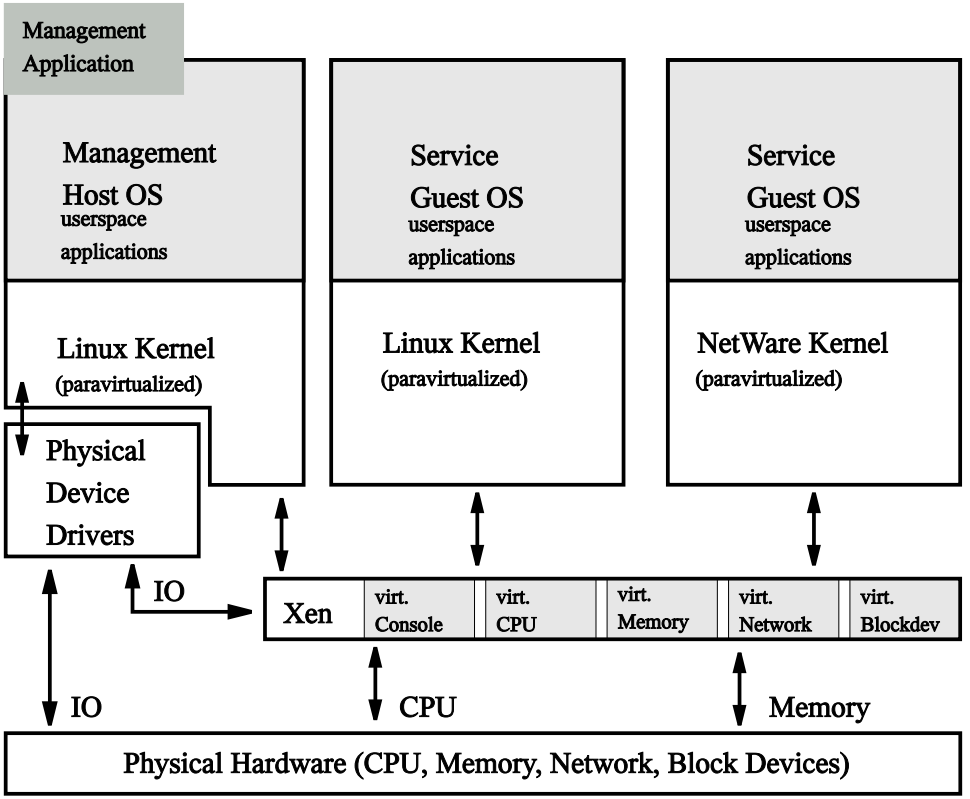
O sistema de virtualização do Xen também tem algumas desvantagens relativas ao hardware suportado:

- Vários drivers de código-fonte fechado, como os da Nvidia ou ATI, não funcionam como esperado. Nesses casos, você deve usar os drivers de código-fonte aberto se disponíveis, mesmo que eles não suportem as capacidades totais dos chips. Além disso, vários chips de WLAN e pontes cardbus não são suportados durante o uso do Xen.

- Na versão 2, o Xen não suporta PAE (extensão de endereço físico), significando que ele não suporta mais do que 4 GB de memória.

- Não há suporte para ACPI. O gerenciamento de energia e outros modos que dependem da ACPI não funcionam.

Figura 37.1 *Visão geral do Xen*



37.1 Instalação do Xen

O procedimento de instalação do Xen envolve a configuração de um domínio domain-0 e a instalação de clientes do Xen. Primeiro, verifique se os pacotes necessários estão instalados. Esses são `python`, `bridge-utils`, `xen` e um pacote `kernel-xen`. Ao usar pacotes do SUSE, o Xen é adicionado à configuração do GRUB. Para outros casos, digite uma entrada em `boot/grub/menu.lst`. Essa entrada deve ser similar ao seguinte:

```
title Xen2
    kernel (hd0,0)/boot/xen.gz dom0_mem=458752
    module (hd0,0)/boot/vmlinuz-xen <parameters>
    module (hd0,0)/boot/initrd-xen
```

Substitua (hd0,0) pela partição que mantém o seu diretório `/boot`. Consulte também o Capítulo 29, *O Carregador de Boot* (p 453). Mude a quantidade ded dom0_mem para corresponder ao seu sistema. O valor máximo é a memória do seu sistema em kB menos 65536. Substitua <parameters> pelos parâmetros normalmente usados para inicializar um kernel do Linux. Em seguida, reinicialize no modo Xen. Isso inicializa o hypervisor do Xen e um kernel do Linux levemente modificado como Domain-0 que executa a maioria do hardware. Além das exceções já mencionadas, tudo deve funcionar normalmente.

37.2 Instalação do domínio

A instalação e a configuração de um domínio convidado envolve vários procedimentos. No exemplo a seguir, um primeiro domínio convidado é instalado e todas as tarefas diferentes para criar uma primeira conexão de rede são concluídas.

Para instalar um sistema convidado, você deve fornecer um sistema de arquivos root em um dispositivo de bloco ou em uma imagem de sistema de arquivos, que precisa ser configurado. Para acessar o sistema mais tarde, use um console emulado ou configure a conexão de rede para este convidado. A instalação do SUSE Linux em um diretório é suportada pelo YaST. Os requisitos de hardware de tal convidado são similares a uma instalação normal do Linux.

Domínios podem compartilhar sistemas de arquivos que são montados somente leitura de todos os domínios, como `/usr` ou `/opt`. Nunca compartilhe um sistema de arquivos que é montado como leitura e gravação. Para compartilhar dados graváveis em vários domínios convidados, use o NFS ou outros sistemas de arquivos de rede ou do cluster.

ATENÇÃO: Iniciando um domínio convidado

Ao iniciar um domínio convidado, verifique se os sistemas de arquivos do convidado não estejam mais montados por um instalador ou pelo domain-0 controlador.

A primeira ação é criar uma imagem do sistema de arquivos no qual o Linux para o convidado está instalado:

1. Para criar uma imagem vazia chamada `guest1` no diretório `/var/tmp/` de 4 GB de tamanho, use o comando a seguir:

```
dd if=/dev/zero of=/var/tmp/guest1 seek=1M bs=4096 count=1
```

2 A imagem é um arquivo grande vazio sem informações. Para poder gravar arquivos nele, um sistema de arquivos é necessário:

```
mkreiserfs -f /var/tmp/guest1
```

O comando `mkreiserfs` informa que este não é um dispositivo especial de bloco e pede uma confirmação. Digite Y e Enter para continuar.

3 A instalação real é feita em um diretório. Desta forma, a imagem do sistema de arquivos `/var/tmp/guest1` deve ser montada em um diretório:

```
mkdir -p /var/tmp/dirinstall
mount -o loop /var/tmp/guest1 /var/tmp/dirinstall
```

IMPORTANTE

Quando tiver terminado a instalação, desmonte essa imagem de sistema de arquivos novamente. O YaST também monta o sistema de arquivos `/proc` durante a instalação, que deve ser desmontado também:

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall
```

37.2.1 Usando o YaST para instalar um domínio convidado

Para instalar um domínio convidado com o YaST, você precisa da imagem do sistema de arquivos previamente preparado para o novo convidado. Inicie o YaST e selecione *Software → Instalação no Diretório para XEN*.

O módulo YaST para a instalação do diretório tem várias opções que devem ser definidas de acordo com suas necessidades:

- Diretório de destino: `/var/tmp/dirinstall`

  Defina esta opção para o ponto de montagem da imagem do sistema de arquivos a ser usado. O padrão é geralmente aceitável.

- Executar YaST e SuSEconfig após primeiro boot: Sim

Defina essa opção para *Sim*. Você será solicitado a digitar uma senha de root e um primeiro usuário ao iniciar o convidado pela primeira vez.

- Criar imagem: Não

  A imagem criada é somente um arquivo tar do diretório de instalação. Isso não é útil aqui.

- Software

  Selecione o tipo de instalação a ser usada. Qualquer um dos padrões é um bom começo.

Clique em *Avançar* para iniciar a instalação. Dependendo do número de pacotes, a instalação pode ser um pouco demorada. Após a conclusão da instalação, as bibliotecas tls devem ser movidas:

```
mv /var/tmp/dirinstall/lib/tls /var/tmp/dirinstall/lib/tls.disabled
```

O Xen usa um dos kernels instalados no domain-0 para iniciar o domínio convidado. Para poder usar a rede no convidado, os módulos deste kernel devem estar disponíveis para o convidado também.

```
cp -a /lib/modules/$(rpm -qf --qf %{VERSION}-%{RELEASE}-xen \
    /boot/vmlinuz-xen) /var/tmp/dirinstall/lib/modules
```

Para evitar erros no sistema de arquivos, a imagem de sistema de arquivos deve ser desmontada após a instalação:

```
umount /var/tmp/dirinstall/proc
umount /var/tmp/dirinstall/
```

Seria possível criar kernels especializados para o domain-0 em uma extremidade e para os sistemas convidados na outra extremidade. A diferença principal são os drivers do hardware que são desnecessários em sistemas convidados. Como esses drivers são modulares e não usados em sistemas convidados, o SUSE entrega somente um kernel para ambas as tarefas.

37.2.2 Configurando um sistema de resgate para funcionar como um domínio convidado

A maneira mais fácil de executar um sistema rapidamente é reutilizar um sistema de arquivos raiz existente, como o sistema de resgate do SUSE Linux. Basicamente, troque a imagem de kernel e os drivers do dispositivo do bloco virtual e dispositivos de rede nesta imagem. Para facilitar esta tarefa, o script `mk-xen-rescue-img.sh` está disponível em `/usr/share/doc/packages/xen/`.

A desvantagem de usar o método de resgate para criar um sistema de arquivos raiz é que o resultado não tem um banco de dados RPM, então você não pode adicionar pacotes facilmente usando RPM. No lado positivo, o resultado é relativamente pequeno, mas tem praticamente tudo o que é necessário para iniciar a rede.

Para executar o script `mk-xen-rescue-img.sh`, você precisa de pelo menos o diretório com a imagem de resgate e um local de destino para a imagem resultante. Por padrão, o diretório reside no DVD de boot no diretório `/boot`.

```
cd /usr/share/doc/packages/xen
./mk-xen-rescue-img.sh /media/dvd/boot /usr/local/xen 64
```

O primeiro parâmetro do script é o diretório da imagem de resgate. O segundo parâmetro é o destino do arquivo de imagem. Parâmetros opcionais são os requisitos de espaço em disco do domínio convidado recém-gerado e a versão de kernel a ser usada.

Em seguida, o script copia a imagem para o novo local, substitui o kernel e vários módulos de kernel e desabilita o diretório `tls` no sistema. Como última etapa, ele gera um arquivo de configuração para a nova imagem em `/etc/xen/`.

37.3 Configurando um domínio convidado do Xen

A documentação sobre como configurar um domínio convidado não é muito completa. A maioria das informações sobre como configurar tal domínio pode ser encontrada no arquivo de configuração de exemplo `/etc/xen/config`. As opções necessárias são explicadas junto com o valor padrão ou pelo menos uma configuração de exemplo.

Para a instalação descrita na Seção 37.2.1, “Usando o YaST para instalar um domínio convidado” (p 577), crie um arquivo `/etc/xen/guest1` com o seguinte conteúdo:

```
kernel = "/boot/vmlinuz-xen"                    ❶
ramdisk = "/boot/initrd-xen"                    ❷
memory = 128                                    ❸
name = "guest1"                                 ❹
nics = "1"                                      ❺
vif = [ 'mac=aa:cc:00:00:00:ab, bridge=xen-br0' ] ❻
disk = [ 'file:/var/tmp/guest1,hda1,w' ]        ❼
root = "/dev/hda1 ro"                           ❽
extra = "3"                                     ❾
```

❶ Digite o caminho para o kernel do Xen no domain-0. Este kernel será executado no sistema convidado mais tarde.

❷ Selecione o disco de RAM inicial apropriado que contém os drivers do dispositivo para o kernel do Xen. Sem isso, o kernel geralmente falha, pois não é capaz de montar seu sistema de arquivos raiz.

❸ Defina a quantidade de memória que deve ser fornecida ao domínio convidado. Isso falhará se o sistema não tiver memória suficiente disponível para os convidados.

❹ O nome para esse convidado.

❺ O número de interfaces de rede virtual para o domínio convidado.

❻ A configuração da interface de rede virtual, incluindo seu endereço MAC e a ponte à qual está conectada.

❼ Defina os dispositivos de bloco virtual para o convidado do Xen. Para usar dispositivos de bloco reais, crie entradas como `['phy:sdb1,hda1,w', 'phy:system/swap1,hda2,w']`.

❽ Define o dispositivo raiz para o kernel. Esse deve ser o dispositivo virtual conforme visto pelo convidado.

❾ Adicione parâmetros de kernel extra aqui. O exemplo `3` significa que o convidado é iniciado no nível de execução 3.

37.4 Iniciando e controlando domínios do Xen

Antes que o domínio convidado possa ser iniciado, o hypervisor do Xen deve ter memória livre suficiente para o novo convidado. Primeiro, verifique a quantidade de memória usada:

```
xm list
Name              Id  Mem(MB)  CPU  State  Time(s)  Console
Domain-0           0      458    0  r----    181.8
```

Se este for um computador com 512 MB, o hypervisor do Xen usa 64 MB e o Domain-0 ocupa o restante. Para liberar parte da memória para o novo convidado, o comando `xm balloon` será usado. Para definir o tamanho do Domain-0 para 330 MB, digite o seguinte como `root`:

```
xm balloon 0 330
```

Na próxima `xm list`, o uso de memória de Domain-0 deverá ter diminuído para 330 MB. Agora há memória suficiente disponível para iniciar um convidado com 128 MB. O comando `xm start guest1 -c` inicia o convidado e vincula o console do convidado inicial ao terminal atual. Se esta for a primeira vez em que esse convidado é iniciado, termine a instalação com o YaST.

Sempre é possível destacar esse console ou reconectá-lo de outro terminal. Para destacá-lo, use Ctrl +]. Para reconectá-lo, primeiro verifique o ID do convidado necessário com `xm list` e conecte-o ao ID com `xm console` *`ID`*.

A ferramenta xm do Xen tem vários parâmetros possíveis. Exiba uma lista com uma explicação curta digitando `xm help`. A Tabela 37.1, “Comandos xm” (p 581) fornece alguns dos comandos mais importantes como ponto de início.

Tabela 37.1 *Comandos xm*

`xm help`	Imprima uma lista de comandos disponíveis para a ferramenta xm.
`xm console` *`ID`*	Conecte ao primeiro console (tty1) do convidado com o ID *`ID`*.

`xm balloon` *`ID Mem`*	Defina o tamanho da memória do domínio com o ID *`ID`* para *`Mem`* em MB.
`xm create` *`domname`* `[-c]`	Inicie o domínio com o arquivo de configuração *`domname`*. O `-c` opcional vincula o terminal atual ao primeiro tty do novo convidado.
`xm shutdown` *`ID`*	Realize um encerramento normal do convidado com o ID *`ID`*.
`xm destroy` *`ID`*	Termine o convidado com ID *`ID`* imediatamente.
`xm list`	Imprima uma lista de todos os domínios em execução com o ID respectivo, a memória e os valores de tempo de CPU.
`xm info`	Exiba informações sobre o host do Xen, incluindo informações de memória e CPU.

37.5 Para obter mais informações

Mais informações sobre o Xen podem ser encontradas nos seguintes sites:

- `file:/usr/share/doc/packages/xen/user/html/index.html`—Informações oficiais para usuários do Xen. Exige o pacote `xen-doc-html`.
- `file:/usr/share/doc/packages/xen/interface/html/index.html`—Mais documentação de interface técnica. Também exige o pacote `xen-doc-html`.
- `http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html`—Home page do Xen com vários links de documentação diferentes.
- `http://lists.xensource.com/`—Várias listas de discussão sobre o Xen.

Parte IX Serviços

38 Rede básica

O Linux oferece os recursos e as ferramentas de rede necessários para a integração em todos os tipos de estruturas de rede. O protocolo Linux comum, TCP/IP, possui vários serviços e recursos especiais abordados aqui. O acesso à rede através de placa de rede, modem ou outro dispositivo pode ser configurado com o YaST. A configuração também pode ser feita manualmente. Somente os mecanismos fundamentais e os arquivos de configuração de rede relevantes serão discutidos neste capítulo.

Linux e outros sistemas operacionais Unix usam o protocolo TCP/IP. Não é um protocolo de rede único, mas uma família de protocolos de rede que oferece vários serviços. Os protocolos listados na Tabela 38.1, “Vários protocolos na família de protocolos TCP/IP” (p 586) são fornecidos com a finalidade de trocar dados entre duas máquinas através do TCP/IP. A redes combinadas por TCP/IP compõem uma rede mundial também chamada de “Internet.”

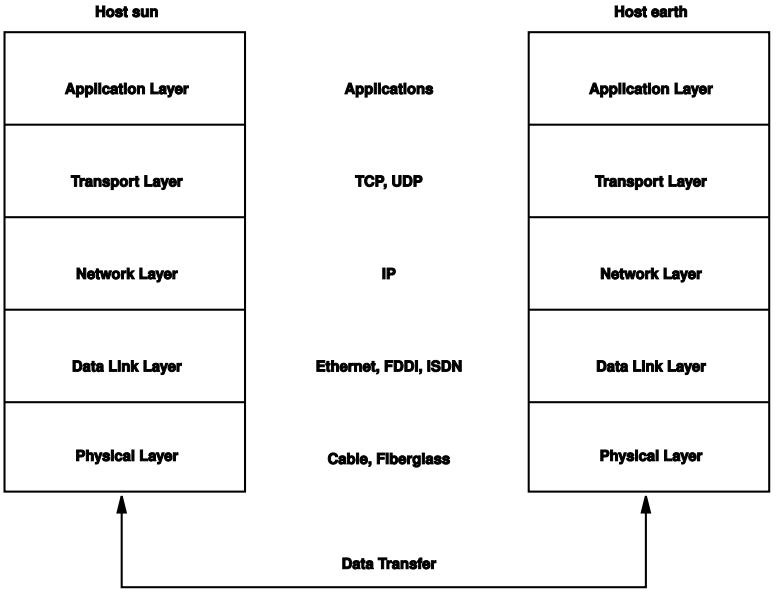
RFC significa *Request for Comments*. Os RFCs são documentos que descrevem vários procedimentos de implementação e protocolos da Internet para o sistema operacional e seus aplicativos. Os documentos RFC descrevem a configuração dos protocolos da Internet. Para ampliar seu conhecimento sobre qualquer dos protocolos, consulte os documentos de RFC apropriados. Eles estão disponíveis online em `http://www.ietf.org/rfc.html`.

Tabela 38.1 *Vários protocolos na família de protocolos TCP/IP*

Protocolo	Descrição
TCP	Protocolo de controle de transmissão: um protocolo seguro orientado por conexão. Os dados a serem transmitidos são primeiramente enviados pelo aplicativo como um fluxo de dados. Depois, são convertidos pelo sistema operacional no formato apropriado. Os dados chegam ao respectivo aplicativo no host de destino no formato do fluxo de dados original no qual foram inicialmente enviados. O TCP determina se algum dado foi perdido durante a transmissão e se não foram misturados. O TCP é implementado onde a seqüência de dados for necessária.
UDP	UDP: um protocolo inseguro, sem conexão. Os dados a serem transmitidos são enviados na forma de pacotes gerados pelo aplicativo. A ordem em que os dados chegam ao destinatário não é garantida e eles podem ser perdidos. O UDP é adequado para aplicativos orientados por registro. Ele possui um período de latência menor que o TCP.
ICMP	ICMP: essencialmente, não é um protocolo para o usuário final, mas um protocolo de controle especial que emite relatórios de erros e pode controlar o comportamento de máquinas que participam da transferência de dados TCP/IP. Além disso, ele fornece um modo de eco especial, que pode ser visualizado usando o programa ping.
IGMP	IGMP: este protocolo controla o comportamento da máquina durante o multicast IP.

Conforme mostrado na Figura 38.1, “Modelo de camadas simplificado para TCP/IP” (p 587), a troca de dados ocorre em camadas diferentes. A camada de rede real é a transferência de dados insegura por IP. Acima do IP, o TCP garante, até certo ponto, a segurança na transferência de dados. A camada IP é suportada pelo protocolo dependente de hardware subjacente, como uma ethernet.

Figura 38.1 *Modelo de camadas simplificado para TCP/IP*



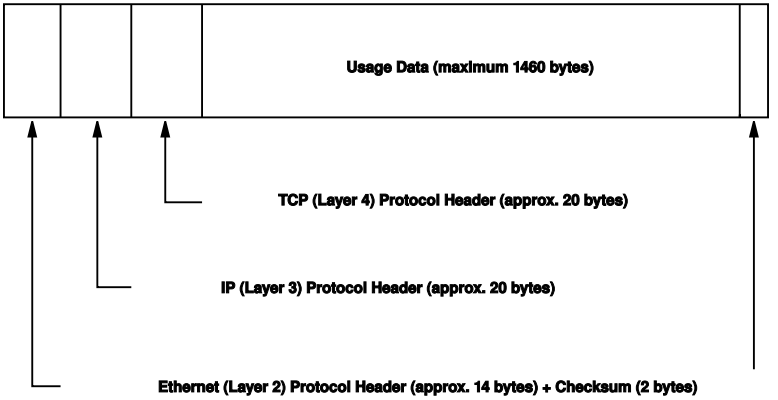
O diagrama fornece um ou dois exemplos para cada camada. As camadas são organizadas de acordo com os *níveis de abstração*. A camada mais baixa fica muito próxima do hardware. A camada mais alta é quase completamente abstraída do hardware. Todas as camadas possuem suas funções especiais próprias. As funções especiais de cada camada, na maioria das vezes, estão implícitas em suas descrições. O link de dados e as camadas físicas representam a rede física usada, como uma ethernet.

Quase todos os protocolos de hardware funcionam em uma base orientada por pacotes. Os dados a serem transmitidos são fornecidos em *pacotes*, pois não podem ser enviados todos de uma vez. O tamanho máximo de um pacote TCP/IP é de, aproximadamente, 64 KB. Os pacotes são normalmente um pouco menores, pois o hardware da rede pode ser um fator de limitação. O tamanho máximo de um pacote de dados em uma ethernet é em torno de 1.500 bytes. O tamanho de um pacote TCP/IP limita-se a esse máximo quando os dados são enviados por uma ethernet. Se mais dados forem transferidos, mais pacotes de dados precisarão ser enviados pelo sistema operacional.

Para que as camadas executem suas respectivas funções, informações adicionais referentes a cada uma delas devem ser gravadas no pacote de dados. Isso ocorre no *cabeçalho* do pacote. Todas as camadas anexam um pequeno bloco de dados, chamado cabeçalho do protocolo, à frente de cada pacote emergente. Um exemplo de um pacote

de dados TCP/IP transmitido por um cabo ethernet é exibido na Figura 38.2, “Pacote Ethernet TCP/IP” (p 588). A soma de teste está localizada no final do pacote e não no início. Isso torna as coisas mais simples para o hardware de rede.

Figura 38.2 *Pacote Ethernet TCP/IP*


Usage Data (maximum 1460 bytes)
TCP (Layer 4) Protocol Header (approx. 20 bytes)
IP (Layer 3) Protocol Header (approx. 20 bytes)
Ethernet (Layer 2) Protocol Header (approx. 14 bytes) + Checksum (2 bytes)

Quando um aplicativo envia dados por uma rede, eles passam por cada camada, todas implementadas no kernel do Linux, exceto a camada física. Cada camada é responsável pela preparação dos dados, para que eles possam passar para a camada seguinte. A camada mais baixa é a responsável pelo envio de dados. Todo o processo é invertido quando os dados são recebidos. Como camadas de uma cebola, em cada uma os cabeçalhos de protocolo são removidos dos dados transportados. Por fim, a camada de transporte é responsável por disponibilizar os dados para uso pelos aplicativos de destino. Dessa forma, cada camada se comunica somente com a camada diretamente acima ou abaixo dela. Para os aplicativos, é relevante se os dados são transmitidos através de uma rede FDDI de 100 MBit/s ou de uma linha de modem de 56 kbit/s. Da mesma forma, é relevante para a linha de dados os tipos de dados transmitidos, contanto que os pacotes estejam no formato correto.

38.1 Roteamento e endereços IP

Esta seção limita-se à abordagem de redes IPv4. Para obter informações sobre o protocolo IPv6, sucessor do IPv4, consulte a Seção 38.2, “IPv6— A Internet da próxima geração” (p 591).

38.1.1 Endereços IP

Todo computador na Internet possui um endereço de 32 bits exclusivo. Esses 32 bits (ou 4 bytes) são normalmente gravados conforme ilustrado na segunda linha no Exemplo 38.1, “Gravando endereços IP” (p 589).

Exemplo 38.1 *Gravando endereços IP*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Na forma decimal, os quatro bytes são gravados no sistema de números decimais, separados por pontos. O endereço IP é designado a um host ou a uma interface de rede. Ele não pode ser usado em nenhum outro lugar no mundo. Há exceções a essa regra, mas não são relevantes nas passagens a seguir.

Os pontos nos endereços IP indicam o sistema hierárquico. Até os anos 90, os endereços IP eram estritamente categorizados em classes. Entretanto, esse sistema provou ser excessivamente inflexível e foi interrompido. Agora, o *CIDR* (Classless Interdomain Routing - Roteamento Interdomínio sem Classes) é usado.

38.1.2 Máscaras de rede e roteamento

As máscaras de rede são usadas para definir a faixa de endereços de uma sub-rede. Se dois hosts estão em uma mesma sub-rede, eles podem se encontrar diretamente. Caso não estejam na mesma sub-rede, precisam do endereço de gateway que controla todo o tráfego entre a sub-rede e o resto do mundo. Para verificar se dois endereços IP estão em uma mesma sub-rede, basta “E” os dois endereços com a máscara de rede. Se o resultado for idêntico, os dois endereços IP estarão na mesma rede local. Se houver diferenças, o endereço IP remoto e, portanto, a interface remota, só poderão ser localizados através de um gateway.

Para compreender como as máscaras de rede funcionam, consulte a Exemplo 38.2, “Vinculando endereços IP à máscara de rede” (p 590). A máscara de rede consiste em 32 bits que identificam quanto de um endereço IP pertence à rede. Todos os bits `1` marcam o bit correspondente no endereço IP como pertencente à rede. Todos os bits `0` marcam os bits dentro da sub-rede. Isso significa que quanto maior a quantidade de bits `1`, menor será o tamanho da sub-rede. Como a máscara de rede sempre consiste em vários bits `1` sucessivos, também é possível apenas contar o número de bits da máscara

de rede. Na Exemplo 38.2, “Vinculando endereços IP à máscara de rede” (p 590) a primeira rede com 24 bits também poderia ser gravada como `192.168.0.0/24`.

Exemplo 38.2 *Vinculando endereços IP à máscara de rede*

```
IP address (192.168.0.20): 11000000 10101000 00000000 00010100
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Para dar outro exemplo: todas as máquinas conectadas ao mesmo cabo ethernet, normalmente, estão localizadas na mesma sub-rede e são diretamente acessíveis. Mesmo quando a sub-rede é dividida fisicamente por switches ou pontes, esses hosts ainda assim podem ser diretamente localizados.

Endereços IP fora da sub-rede local só poderão ser localizados se um gateway for configurado para a rede de destino. Nos casos mais comuns, há somente um gateway que controla todo o tráfego externo. Entretanto, também é possível configurar vários gateways para sub-redes diferentes.

Se um gateway tiver sido configurado, todos os pacotes IP externos serão enviados para o gateway apropriado. Esse gateway tentará então encaminhar os pacotes da mesma forma (de host para host) até acessar o host de destino ou até o TTL (time to live) do pacote expirar.

Tabela 38.2 *Endereços específicos*

Tipo de endereço	Descrição
Endereço de rede de base	Essa é a máscara de rede E qualquer endereço na rede, conforme mostrado na Exemplo 38.2, “Vinculando endereços IP à máscara de rede” (p 590) em `Resultado`. Esse endereço não pode ser designado a nenhum host.
Endereço de broadcast	Isso significa, basicamente, “Acessar todos os hosts nesta sub-rede.” Para gerar isso, a máscara de rede é invertida no formato

Tipo de endereço	Descrição
	binário e vinculada ao endereço de rede base com um OU lógico. O exemplo acima resulta, portanto, em 192.168.0.255. Esse endereço não pode ser designado a nenhum host.
Host local	O endereço `127.0.0.1` é designado ao "dispositivo loopback" em cada host. Uma conexão pode ser configurada em sua própria máquina com esse endereço.

Como os endereços IP precisam ser exclusivos em qualquer parte do mundo, não é possível selecionar endereços aleatoriamente. Há três domínios de endereços a serem usados para configurar uma rede baseada em IP privado. Eles não conseguem se conectar ao restante da Internet, pois não podem ser transmitidos através dela. Esses domínios de endereço são especificados no RFC 1597 e listados na Tabela 38.3, "Domínios de endereços IP privados" (p 591).

Tabela 38.3 *Domínios de endereços IP privados*

Rede/máscara de rede	Domínio
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

38.2 IPv6— A Internet da próxima geração

Devido ao surgimento da WWW (World Wide Web), a Internet teve um crescimento explosivo com um número cada vez maior de computadores se comunicando através de TCP/IP nos últimos quinze anos. Desde que Tim Berners-Lee da CERN (`http://public.web.cern.ch`) inventou a WWW em 1990, o número de hosts da Internet cresceu de poucos milhares para centenas de milhões deles.

Conforme mencionado, um endereço IPv4 consiste em apenas 32 bits. Da mesma forma, poucos endereços IP são perdidos — eles não podem ser usados devido à forma como as redes são organizadas. O número de endereços disponíveis na sua sub-rede é dois elevado à potência do número de bits, menos dois. Uma sub-rede tem, por exemplo, 2, 6 ou 14 endereços disponíveis. Para conectar 128 hosts à Internet, por exemplo, você precisa de uma sub-rede com 256 endereços IP, dos quais somente 254 são utilizáveis, pois dois endereços IP são necessários para a estrutura da própria sub-rede: o endereço da rede de base e broadcast.

No protocolo IPv4 atual, DHCP ou NAT (Network Address Translation - Conversão de Endereços de Rede) são os mecanismos comuns usados para contornar a grande falta de endereços. Combinado à convenção de manter endereços públicos e privados separados por espaços, esses métodos podem certamente reduzir a falta de endereços. O problema deles está em suas configurações, trabalhosas para configurar e difíceis de manter. Para configurar um host em uma rede IPv4, é preciso haver vários itens de endereços, como o próprio endereço IP do host, a máscara de sub-rede, o endereço de gateway e talvez o endereço do servidor de nomes. Todos esses itens precisam ser conhecidos e não podem ser derivados de outro lugar.

Com o IPv6, tanto a falta de endereços quanto as configurações complicadas passariam a ser problemas do passado. As seções a seguir oferecem mais informações sobre os aprimoramentos e benefícios trazidos pelo IPv6 e sobre a transição do protocolo antigo para o novo.

38.2.1 Vantagens

A melhoria mais importante e visível oferecida pelo novo protocolo é a expansão enorme do espaço disponível para endereços. Um endereço IPv6 é criado com valores de 128 bits em vez dos 32 bits tradicionais. Ele é capaz de fornecer 'quatrilhões' de endereços IP.

Entretanto, os endereços IPv6 não diferem de seus antecessores apenas em relação ao comprimento. Também possuem uma estrutura interna diferente, que pode conter mais informações específicas sobre os sistemas e as redes a que pertencem. Leia mais detalhes sobre eles na Seção 38.2.2, “Estrutura e tipos de endereços” (p 594).

A seguir, há uma lista de algumas outras vantagens do novo protocolo:

Configuração automática

O IPv6 torna apto o "plug and play" da rede, o que significa que um sistema recentemente configurado é integrado à rede (local) sem qualquer configuração manual. O novo host usa seu mecanismo de configuração automática para derivar seu próprio endereço a partir das informações disponibilizadas pelos roteadores vizinhos, com base em um protocolo chamado protocolo *ND* (Neighbor Discovery - Descoberta de Vizinho). Esse método não exige nenhuma intervenção por parte do administrador e não há necessidade de manter um servidor central para alocação de endereços; uma vantagem adicional em relação ao IPv4, cuja alocação automática de endereços exige um servidor DHCP.

Mobilidade

O IPv6 torna possível a designação de vários endereços a uma interface de rede ao mesmo tempo. Isso permite que usuários acessem várias redes facilmente, o que é comparado aos serviços de roaming internacionais oferecidos pelas empresas de celulares: quando você viaja com seu celular, ele automaticamente se conecta a um serviço interurbano, assim que entra na área correspondente. Dessa forma, você pode ser localizado no mesmo número de celular em qualquer lugar e pode fazer ligações como se estivesse em sua cidade.

Comunicação segura

Com o IPv4, a segurança da rede é uma função adicional. O IPv6 inclui IPSec como um de seus recursos principais, permitindo que sistemas se comuniquem através de um túnel seguro, para evitar a intromissão de estranhos na Internet.

Compatibilidade retroativa

De forma realista, seria impossível mudar toda a Internet de IPv4 para IPv6 de uma só vez. Portanto, é essencial que ambos os protocolos sejam capazes de coexistir na Internet, mas também em um sistema. Isso é garantido por endereços compatíveis (endereços IPv4 podem facilmente ser convertidos em endereços IPv6) e através do uso de vários túneis. Consulte a Seção 38.2.3, "Coexistência de IPv4 e IPv6" (p 599). Da mesma forma, os sistemas podem se basear em uma técnica *IP de pilha dupla* para suportar os dois protocolos ao mesmo tempo, significando que possuem duas pilhas de rede completamente separadas, de tal forma que não há interferência entre as duas versões de protocolos.

Serviços adaptados e personalizados através de Multicast

Com o IPv4, alguns serviços, como SMB, precisam transmitir seus pacotes para todos os host na rede local. O IPv6 oferece uma abordagem mais detalhada, permitindo que os servidores enviem hosts através de *multicast* — determinando

um número de hosts como partes de um grupo (diferente de direcionar todos os hosts através de *broadcast* ou cada host individualmente através de *unicast*). Os hosts enviados como grupos talvez dependam do aplicativo concreto. É possível enviar todos os servidores de nomes para alguns grupos predefinidos (o *grupo multicast de servidores de nomes*), por exemplo ou todos os roteadores (o *grupo multicast de todos os roteadores*).

38.2.2 Estrutura e tipos de endereços

Como mencionado, está faltando no protocolo IP atual dois aspectos importantes: há um aumento de falta de endereços IP e a configuração de rede e manutenção de tabelas de roteamento vêm se tornando tarefas cada vez mais complexas e trabalhosas. O IPv6 soluciona o primeiro problema, expandindo o espaço dos endereços para 128 bits. O segundo problema é contornado com a introdução de uma estrutura hierárquica de endereços, combinada com técnicas sofisticadas para alocar endereços de rede, assim como *multihoming* (a capacidade de designar vários endereços a um dispositivo, permitindo acesso a diversas redes).

Ao utilizar o IPv6, é útil saber que há três tipos diferentes de endereços:

Unicast
: Endereços desse tipo são associados com exatamente uma interface de rede. Pacotes com esse tipo de endereço são entregues em apenas um destino. Da mesma forma, os endereços unicast são usados para transferir pacotes para hosts individuais na rede local ou na Internet.

Multicast
: Endereços desse tipo estão relacionados a um grupo de interfaces de rede. Pacotes com esse tipo de endereço são entregues a todos os destinos pertencentes ao grupo. Endereços multicast são usados, principalmente, por certos tipos de serviços de rede para se comunicarem com determinados grupos de host de forma bem direcionada.

Anycast
: Endereços desse tipo estão relacionados a um grupo de interfaces. Pacotes com esse tipo de endereço são entregues ao membro do grupo mais próximo do remetente, de acordo com os princípios do protocolo de roteamento subjacente. Endereços anycast são usados para que hosts possam descobrir mais facilmente servidores que oferecem certos serviços na área da rede determinada. Todos os servidores do mesmo tipo possuem o mesmo endereço anycast. Sempre que um host solicita um serviço,

ele recebe uma resposta do servidor com o local mais próximo, conforme determinado pelo protocolo de roteamento. Caso ocorra alguma falha com esse servidor, o protocolo selecionará automaticamente o segundo servidor mais próximo ou então o terceiro e assim por diante.

Um endereço IPv6 é constituído de oito campos de quatro dígitos, cada um representando 16 bits, gravados em notação hexadecimal. Também são separados por dois-pontos (`:`). Quaisquer zero bytes iniciais em um determinado campo podem ser descartados, mas zeros dentro ou no final do campo não podem ser descartados. Outra convenção é a de que mais de quatro zero bytes consecutivos podem retornar como dois-pontos duplos. Entretanto, somente um como `::` é permitido em cada endereço. Esse tipo de notação reduzida é mostrado no Exemplo 38.3, "Amostra de endereço IPv6" (p 595), em que todas as três linhas representam o mesmo endereço.

Exemplo 38.3 *Amostra de endereço IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Cada parte de um endereço IPv6 possui uma função definida. Os primeiros bytes formam o prefixo e especificam o tipo de endereço. A parte central é a porção do endereço na rede, mas pode não ser utilizada. O final do endereço forma a parte do host. Com o IPv6, a máscara de rede é definida indicando o comprimento do prefixo depois de uma barra no final do endereço. Um endereço, como mostrado no Exemplo 38.4, "Endereço IPv6 especificando o comprimento do prefixo" (p 595), contém as informações de que os primeiros 64 bits formam a parte da rede do endereço e que os últimos 64 formam a parte do host. Em outras palavras, `64` significa que a máscara de rede está preenchida com 64 valores de 1 bit a partir da esquerda. Da mesma forma que o IPv4, o endereço IP é combinado com E com os valores da máscara de rede, para determinar se o host está localizado na mesma sub-rede ou em outra.

Exemplo 38.4 *Endereço IPv6 especificando o comprimento do prefixo*

```
fe80::10:1000:1a4/64
```

O IPv6 conhece vários tipos de prefixos predefinidos. Alguns são mostrados na Tabela 38.4, "Vários prefixos IPv6" (p 596).

Tabela 38.4 *Vários prefixos IPv6*

Prefixo (hex)	Definição
`00`	Endereços IPv4 e endereços de compatibilidade de IPv4 sobre IPv6. Esses são usados para manter a compatibilidade com IPv4. O seu uso ainda exige um roteador capaz de converter pacotes IPv6 em pacotes IPv4. Vários endereços especiais, como o do dispositivo loopback, também possuem esse prefixo.
`2` ou `3` como o primeiro dígito	Endereços unicast globais agregativos. Como no caso do IPv4, uma interface pode ser designada para fazer parte de uma determinada sub-rede. Atualmente, há os seguintes espaços de endereços: `2001::/16` (espaço de endereço da qualidade de produção) e `2002::/16` (espaço de endereço 6to4).
`fe80::/10`	Endereços locais de links. Endereços com esse prefixo não devem ser roteados e, portanto, só devem ser encontrados na mesma sub-rede.
`fe80::/10`	Endereços locais de sites. Esses podem ser roteados, mas somente na rede da organização a que pertencem. Na verdade, eles são o equivalente IPv6 do espaço de endereço de rede privada atual, como `10.x.x.x`.
`ff`	Esses são endereços multicast.

Um endereço unicast consiste em três componentes básicos:

Topologia pública
A primeira parte (que também contém um dos prefixos mencionados acima) é usada para rotear pacotes através da Internet pública. Ela inclui informações sobre a empresa ou instituição que fornece o acesso à Internet.

Topologia do site
A segunda parte contém informações de roteamento sobre a sub-rede à qual o pacote deve ser entregue.

ID de interface
A terceira parte identifica a interface à qual o pacote deve ser entregue. Isso também permite que o MAC faça parte do endereço. Como MAC é um identificador fixo globalmente exclusivo codificado no dispositivo pelo fabricante do hardware, o procedimento de configuração é bastante simplificado. Na verdade, os primeiros 64 bits de endereço são consolidados para formar o token `EUI-64`, com os últimos 48 bits obtidos no MAC e os 24 bits restantes contendo informações especiais sobre o tipo de token. Isso também possibilita designar um token `EUI-64` a interfaces que não possuem MAC, como aquelas baseadas em PPP ou ISDN.

No topo dessa estrutura básica, o IPv6 faz distinção entre cinco tipos de endereços unicast:

`::` (não especificado)
Esse endereço é usado pelo host como seu endereço de origem quando a interface é inicializada pela primeira vez — quando o endereço ainda não pode ser determinado por outros meios.

`::1` (loopback)
O endereço do dispositivo loopback.

Endereços compatíveis com o IPv4
O endereço IPv6 é formado pelo endereço IPv4 e um prefixo consistindo em 96 zero bits. Esse tipo de endereço de compatibilidade é usado para um túnel (consulte a Seção 38.2.3, “Coexistência de IPv4 e IPv6” (p 599)) para permitir que os hosts IPv4 e IPv6 se comuniquem com outros que estejam operando em um ambiente IPv4 puro.

Endereços IPv4 mapeados para IPv6
Esse tipo de endereço especifica um endereço IPv4 puro em uma notação IPv6.

Endereços locais
Há dois tipos de endereços para uso local:

link-local
Esse tipo de endereço só pode ser usado na sub-rede local. Pacotes com endereço de origem ou de destino desse tipo não devem ser roteados para a Internet nem para outras sub-redes. Esses endereços contêm um prefixo especial (`fe80::/10`) e o ID da interface da placa de rede, com a parte do meio consistindo em zero bytes. Endereços desse tipo são usados durante a

configuração automática para se comunicarem com outros hosts pertencentes à mesma sub-rede.

site-local
: Pacotes com esse tipo de endereço podem ser roteados para outras sub-redes, mas não para a Internet mais ampla. Eles precisam permanecer dentro da própria rede da organização. Tais endereços são usados para intranets e equivalem ao espaço de endereço privado definido pelo IPv4. Eles contêm um prefixo especial (`fec0::/10`), o ID da interface e um campo de 16 bits especificando o ID da sub-rede. Novamente, o restante é preenchido com zero bytes.

Como um recurso completamente novo, introduzido com o IPv6, cada interface de rede normalmente obtém vários endereços IP, com a vantagem de que várias redes podem ser acessadas através da mesma interface. Uma dessas redes pode ser totalmente configurada automaticamente usando o MAC e um prefixo conhecido, resultando na possibilidade de todos os hosts na rede local serem encontrados assim que o IPv6 for habilitado (usando o endereço link-local). Com o MAC fazendo parte disso, qualquer endereço IP usado no mundo será exclusivo. As únicas partes variáveis do endereço são aquelas especificando a *topologia do site* e a *topologia pública*, dependendo da rede real na qual o host estiver atualmente operando.

Para que um host avance e retroceda entre duas redes diferentes ele precisa de, pelo menos, dois endereços. Um deles, o *endereço pessoal*, contém não só o ID de interface, como também um identificador da rede doméstica a que ele normalmente pertence (e o prefixo correspondente). O endereço pessoal é um endereço estático e, portanto, normalmente não se modifica. Mesmo assim, todos os pacotes destinados ao host móvel podem ser entregues a ele, independentemente de ele operar na rede doméstica ou em outro local externo. Isso é possível devido aos recursos totalmente novos introduzidos com o IPv6, como *configuração automática sem estado* e *descoberta de vizinho*. Além do endereço residencial, um host móvel obtém um ou mais endereços adicionais pertencentes às redes interurbanas com roaming. Eles são chamados endereços *care-of*. A rede doméstica tem um recurso que encaminha qualquer pacote destinado ao host quando ele está em roaming. Em um ambiente IPv6, essa tarefa é executada pelo *agente local*, que retransmite todos os pacotes destinados ao endereço residencial através de um túnel. Por outro lado, esses pacotes destinados ao endereço care-of são diretamente transferidos para o host móvel sem qualquer desvio especial.

38.2.3 Coexistência de IPv4 e IPv6

A migração de todos os hosts conectados à Internet do IPv4 para o IPv6 é um processo gradual. Os dois protocolos coexistirão durante algum tempo. A coexistência deles em um sistema é garantida onde houver uma implementação de *pilha dupla* de ambos os protocolos. Ainda resta a dúvida de como um host habilitado do IPv6 deve se comunicar com um host IPv4 e como pacotes do IPv6 devem ser transportados pelas redes atuais, que são predominantemente baseadas no IPv4. As melhores soluções oferecem endereços de compatibilidade e túnel (consulte aSeção 38.2.2, “Estrutura e tipos de endereços” (p 594)).

Os hosts do IPv6 relativamente isolados na rede IPv4 (mundial) podem se comunicar através de túneis: Pacotes IPv6 são encapsulados como pacotes IPv4 para serem movidos por uma rede IPv4. Tal conexão entre dois hosts IPv4 é chamada de *túnel*. Para que isso ocorra, os pacotes precisam incluir o endereço de destino do IPv6 (ou o prefixo correspondente), assim como o endereço IPv4 do host remoto no destino final do túnel. Um túnel básico pode ser configurado manualmente, de acordo com um contrato entre os administradores dos hosts. Também é chamado de *túnel estático*.

Entretanto, a configuração e manutenção de túneis estáticos é normalmente muito trabalhosa para ser usada diariamente em comunicações. Portanto, o IPv6 fornece três métodos de *túneis dinâmicos*:

6over4
: Os pacotes IPv6 são automaticamente encapsulados como pacotes IPv4 e enviados por uma rede IPv4 com capacidade multicast. O IPv6 é induzido a considerar toda a rede (Internet) como uma LAN enorme. Com isso, é possível determinar automaticamente o destino final do túnel IPv4. Entretanto, esse método não faz um dimensionamento muito bom e também é dificultado pelo fato de o multicast IP não ser tão difundido na Internet. Portanto, ele apenas fornece uma solução para redes corporativas ou institucionais menores, em que o multicast pode ser habilitado. As especificações para esse método estão descritas no RFC 2529.

6to4
: Com esse método, os endereços IPv4 são automaticamente gerados a partir de endereços IPv6, habilitando a comunicação de hosts IPv6 isolados através de uma rede IPv4. Entretanto, alguns problemas foram relatados no que tange à comunicação entre esses hosts IPv6 isolados e a Internet. O método está descrito no RFC 3056.

Controlador do túnel IPv6
Esse método se baseia em servidores especiais que fornecem túneis dedicados para hosts IPv6. É descrito no RFC 3053.

IMPORTANTE: A Iniciativa 6bone

Nos principais locais "mais estabelecidos" da Internet, já existe uma rede globalmente distribuída de sub-redes IPv6 conectadas através de túneis. Essa é a rede *6bone* (`http://www.6bone.net`), um ambiente de testes IPv6 que pode ser usado por programadores e provedores da Internet que desejam desenvolver e oferecer serviços baseados no IPv6, a fim de obter a experiência necessária para implementar o novo protocolo. Mais informações podem ser encontradas no site desse projeto na Internet.

38.2.4 Configurando o IPv6

Para configurar o IPv6, normalmente não é necessário fazer mudanças nas estações de trabalho individuais. Entretanto, o suporte do IPv6 precisa ser carregado. Para fazer isso, digite `modprobe ipv6` como `raiz`.

Devido ao conceito de configuração automática do IPv6, um endereço é designado à placa de rede na rede *link-local*. Normalmente, nenhum gerenciamento de tabela de roteamento é feito em uma estação de trabalho. Os roteadores de rede podem ser consultados pela estação de trabalho, usando o *protocolo de anúncios do roteador*, para o qual devem ser implementados um prefixo e gateways. O programa radvd pode ser usado para configurar um roteador IPv6. Esse programa informa às estações de trabalho o prefixo que deve ser usado para os endereços IPv6 e os roteadores. Outra opção é usar zebra para a configuração automática dos dois endereços e roteamento.

Consulte a página de manual do ifup(8) para obter informações sobre como configurar vários tipos de túneis usando os arquivos `/etc/sysconfig/network`.

38.2.5 Mais informações

A visão geral acima não abrange totalmente o tópico do IPv6. Para obter informações mais detalhadas sobre o novo protocolo, consulte os livros e a documentação online a seguir:

http://www.ngnet.it/e/cosa-ipv6.php
Uma série de artigos fornecendo uma introdução explicativa sobre os fundamentos básicos do IPv6. Um bom manual sobre o tópico.

http://www.bieringer.de/linux/IPv6/
Aqui, encontre o Linux IPv6-HOWTO e muitos links relacionados ao tópico.

http://www.6bone.net/
Visite esse site se desejar se juntar a uma rede IPv6 com túnel.

http://www.ipv6.org/
O ponto de partida para tudo relativo ao IPv6.

RFC 2640
Informações fundamentais do RFC sobre o IPv6.

IPv6 Essentials
Um livro que descreve todos os aspectos importantes do tópico é o *IPv6 Essentials* de Silvia Hagen (ISBN 0-596-00125-8).

38.3 Resolução de nomes

O DNS ajuda na designação de um endereço IP a um ou mais nomes e na designação de um nome a um endereço IP. No Linux, essa conversão normalmente é executada por um tipo especial de software chamado bind. A máquina responsável por essa conversão é chamada de *servidor de nomes*. Os nomes criam um sistema hierárquico, no qual cada componente do nome é separado por pontos. A hierarquia de nomes é, entretanto, independente da hierarquia de endereços IP descrita acima.

Considere um nome completo, como `earth.example.com`, gravado no formato `hostname.domain`. Um nome completo, denominado *FQDN* (Fully Qualified Domain Name - Nome de Domínio Totalmente Qualificado), consiste em um nome de host e um nome de domínio (`example.com`). O último também inclui o *TLD* (Top Level Domain - Domínio de Nível Superior (`com`).

A designação TLD tornou-se bastante confusa por razões históricas. Tradicionalmente, nomes de domínio com três letras são usados nos EUA. No resto do mundo, os códigos nacionais ISO de duas letras são o padrão. Além disso, TLDs mais longos foram

introduzidos em 2000, representando certas esferas de atividades (por exemplo, `.info`, `.name`, `.museum`).

No início da Internet (antes de 1990), o arquivo `/etc/hosts` era usado para armazenar os nomes de todas as máquinas representadas na Internet. Isso rapidamente se tornou impraticável, devido ao crescente número de computadores conectados à Internet. Por essa razão, um banco de dados descentralizado foi desenvolvido para armazenar nomes de hosts de uma forma amplamente distribuída. Esse banco de dados, semelhante ao servidor de nomes, não possui os dados pertencentes a todos os hosts na Internet já disponíveis, mas pode encaminhar solicitações a outros servidores de nomes.

A parte superior da hierarquia é ocupada pelos *servidores de nomes raiz*. Esses servidores de nomes raiz gerenciam os domínios de nível superior e são executados pelo NIC (Network Information Center). Cada servidor de nomes raiz conhece os servidores de nomes responsáveis por um determinado domínio de nível superior. Para obter informações sobre NICs de domínio superior, vá para `http://www.internic.net`.

O DNS pode fazer mais do que apenas resolver nomes de hosts. O servidor de nomes também distingue qual host recebe e-mails para um domínio inteiro — o *MX (Mail Exchanger - Servidor de Correio)*.

Para sua máquina resolver um endereço IP, ela precisa pelo menos conhecer um servidor de nomes e seu respectivo endereço IP. É fácil especificar esse servidor de nomes com a ajuda do YaST. Se você tiver uma conexão de discagem por modem, talvez não precise nem mesmo configurar um servidor de nomes manualmente. O protocolo de discagem fornece o endereço do servidor de nomes enquanto a conexão é efetuada. A configuração de acesso ao servidor de nomes com o SUSE Linux é descrita no Capítulo 40, *Domain Name System (Sistema de Nomes de Domínio)* (p 633).

O protocolo `whois` está intimamente relacionado ao DNS. Com esse programa, é possível descobrir rapidamente o responsável por qualquer domínio especificado.

38.4 Configurando uma conexão de rede com o YaST

Há muitos tipos de redes suportadas no Linux. A maioria delas usa nomes de dispositivos diferentes e os arquivos de configuração se espalham por vários locais no sistema de

arquivos. Para obter uma visão geral detalhada dos aspectos da configuração manual de rede, consulte a Seção 38.5, “Configurando uma conexão de rede manualmente” (p 613).

Durante a instalação, o YaST pode ser usado para configurar automaticamente todas as interfaces detectadas. Hardwares adicionais podem ser configurados em qualquer momento após sua instalação no sistema. As seções a seguir descrevem a configuração de rede para todos os tipos de conexões de rede suportadas pelo SUSE Linux.

38.4.1 Configurando a placa de rede com o YaST

Depois de iniciar o módulo, o YaST exibe uma caixa de diálogo da configuração geral da rede. A parte superior mostra uma lista com todas as placas de rede ainda não configuradas. Qualquer placa devidamente detectada é listada com seu nome. Os dispositivos que não puderam ser detectados podem ser configurados com *Outro (não detectado)*, conforme descrito na “Configuração manual de uma placa de rede não detectada” (p 603). Na parte inferior, a caixa de diálogo exibe uma lista dos dispositivos configurados até agora, com seus endereços e tipos de rede. Agora, você pode configurar uma nova placa de rede ou mudar uma configuração existente.

Configuração manual de uma placa de rede não detectada

A configuração de uma placa de rede não detectada (listada em *Outro*) inclui os seguintes itens:

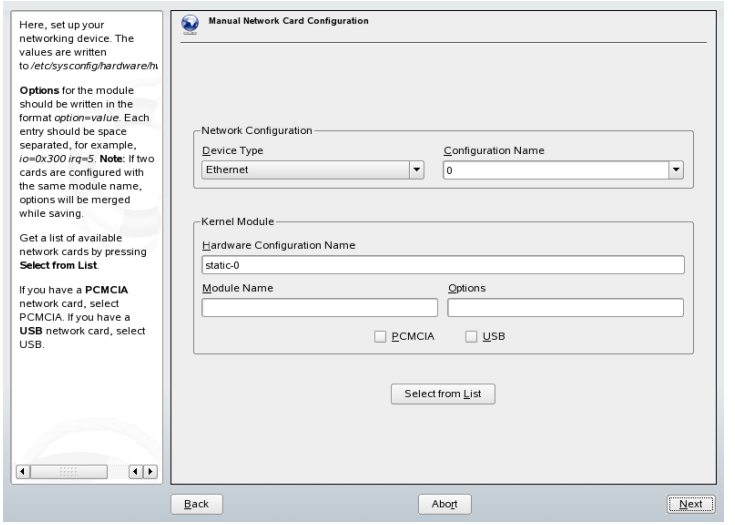
Configuração de rede
Configure o tipo de dispositivo da interface a partir das opções disponíveis e do nome de configuração. As informações sobre as convenções de nomeação para nomes de configuração estão disponíveis na página de manual do `getcfg(8)`.

Módulo de Kernel
Nome de Configuração de Hardware especifica o nome do arquivo `/etc/sysconfig/hardware/hwcfg-*` que contém as configurações de hardware da sua placa de rede. Também contém o nome do módulo de kernel adequado, assim como as opções necessárias para inicializar o hardware. Normalmente, o YaST

sugere nomes úteis para os hardwares PCMCIA e USB. Para outros hardwares, o `hwcfg-static-0` costuma funcionar somente se a placa estiver configurada com o nome de configuração `0`.

Se a placa de rede for um dispositivo PCMCIA ou USB, ative as respectivas caixas de seleção e saia dessa caixa de diálogo com *Próximo*. Caso contrário, selecione o modelo da placa de rede em *Selecionar da Lista*. O YaST selecionará automaticamente o módulo de kernel adequado para a placa. Saia dessa caixa de diálogo com *Próximo*.

Figura 38.3 *Configuração da placa de rede*


Here, set up your networking device. The values are written to /etc/sysconfig/hardware/h
Options for the module should be written in the format option=value. Each entry should be space separated, for example, io=0x300 irq=5. Note: If two cards are configured with the same module name, options will be merged while saving.
Get a list of available network cards by pressing Select from List.
If you have a PCMCIA network card, select PCMCIA. If you have a USB network card, select USB.
Manual Network Card Configuration
Network Configuration
Device Type
Ethernet
Configuration Name
0
Kernel Module
Hardware Configuration Name
static-0
Module Name
Options
PCMCIA
USB
Select from List
Back
Abort
Next

Configurando o endereço de rede

Configure o tipo de dispositivo da interface e o nome da configuração. Selecione o tipo de dispositivo entre os fornecidos. Especifique o nome da configuração de acordo com suas necessidades. Normalmente, as configurações padrão são úteis e podem ser aceitas. As informações sobre as convenções de nomeação para nomes de configuração estão disponíveis na página de manual do `getcfg(8)`.

Se tiver selecionado *Wireless* como tipo de dispositivo da interface, configure o modo operacional, o nome da rede (ESSID) e a criptografia na caixa de diálogo seguinte, *Configuração de Placa de Rede Wireless*. Clique em *OK* para concluir a configuração

da placa. Uma descrição detalhada da configuração de placas WLAN é fornecida na Seção 22.1.3, “Configuração com YaST” (p 308). Para todos os outros tipos de interface, prossiga com a configuração de endereço de rede:

Configuração Automática de Endereço (via DHCP)
: Se sua rede incluir um servidor DHCP, você poderá configurar o endereço de rede com segurança de forma automática. A opção também deverá ser usada se você estiver usando uma linha DSL sem IP estático designado pelo provedor de serviços da Internet. Se decidir usar o DHCP, configure os detalhes depois de selecionar *Opções do Cliente DHCP*. Especifique se o servidor DHCP deve sempre atender a solicitações de broadcast e permitir o uso por qualquer identificador. Por padrão, os servidores DHCP usam o endereço de hardware da placa para identificar uma interface. Se você tiver uma configuração de host virtual, em que hosts diferentes se comunicam através da mesma interface, um identificador será necessário para distingui-los.

Configuração de endereço estático
: Se você possui um endereço estático, habilite essa opção. Depois, digite o endereço e a máscara de sub-rede para sua rede. A máscara de sub-rede predefinida deve corresponder aos requisitos de uma rede doméstica típica.

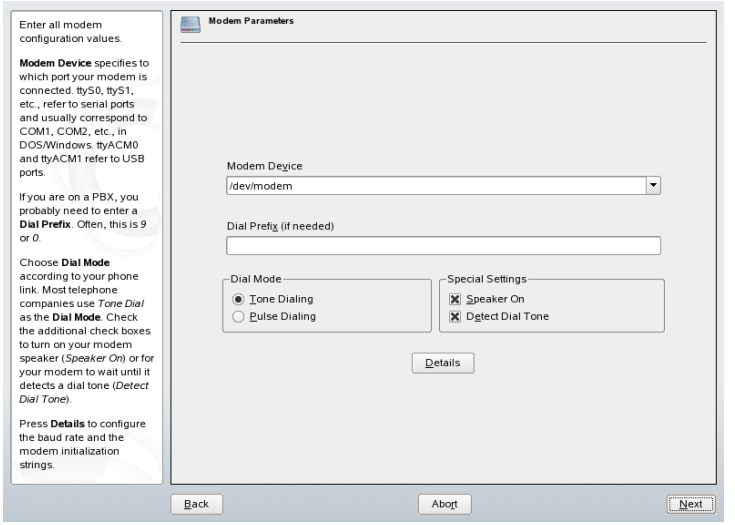
Saia dessa caixa de diálogo, selecionando *Próximo* ou continue a configurar o nome de host, servidor de nomes e detalhes de roteamento (consulte as seções em Servidor DNS (↑Inicialização) e em Roteamento (↑Inicialização)).

Avançado permite especificar configurações mais complexas. Em *Configurações Detalhadas*, use *Controlado pelo Usuário* para delegar o controle sobre a placa de rede desde o administrador (`root`) até o usuário normal. Em operações móveis, isso permite ao usuário adaptar a mudança de conexões de rede de uma forma mais flexível, pois ele pode controlar a ativação ou desativação da interface. A MTU (Maximum Transmission Unit - Unidade de Transmissão Máxima) e o tipo de *Ativação do Dispositivo* também podem ser configurados nessa caixa de diálogo.

38.4.2 Modem

No Centro de Controle do YaST, acesse a configuração do modem em *Dispositivos de Rede*. Se o modem não tiver sido detectado automaticamente, abra a caixa de diálogo e faça uma configuração manual. Na caixa de diálogo aberta, digite a interface à qual o modem está conectado em *Modem*.

Figura 38.4 *Configuração do modem*


Enter all modem configuration values.
Modem Device specifies to which port your modem is connected. ttyS0, ttyS1, etc., refer to serial ports and usually correspond to COM1, COM2, etc., in DOS/Windows. ttyACM0 and ttyACM1 refer to USB ports.
If you are on a PBX, you probably need to enter a Dial Prefix. Often, this is 9 or 0.
Choose Dial Mode according to your phone link. Most telephone companies use Tone Dial as the Dial Mode. Check the additional check boxes to turn on your modem speaker (Speaker On) or for your modem to wait until it detects a dial tone (Detect Dial Tone).
Press Details to configure the baud rate and the modem initialization strings.
Modem Parameters
Modem Device
/dev/modem
Dial Prefix (if needed)
Dial Mode
Tone Dialing
Pulse Dialing
Special Settings
Speaker On
Detect Dial Tone
Details
Back
Abort
Next

Se você estiver usando um PBX, talvez precise digitar um prefixo de discagem. Normalmente, é um zero. Consulte as instruções que acompanham o PBX para descobrir. Selecione também se usará a discagem por tom ou pulso, se o alto-falante estará ligado e se o modem aguardará até detectar um tom de discagem. A última opção não deve ser habilitada se o modem estiver conectado a um intercâmbio.

Em *Detalhes*, configure a taxa de transmissão e as strings de inicialização do modem. Somente mude essas configurações se seu modem não tiver sido detectado automaticamente ou se ele exigir configurações especiais para o funcionamento da transmissão de dados. Esse é basicamente o caso dos adaptadores do terminal ISDN. Saia dessa caixa de diálogo clicando em *OK*. Para delegar controle sobre o modem para um usuário normal, sem permissões de root, ative *Controlado pelo Usuário*. Dessa forma, um usuário sem permissões de administrador poderá ativar ou desativar uma interface. Em *Dial Prefix Expressão Regular*, especifique uma expressão regular. O *Prefixo de Discagem* no KInternet, que pode ser modificado por um usuário normal, precisa corresponder a essa expressão regular. Se esse campo for deixado vazio, o usuário não poderá configurar um *Prefixo de Discagem* diferente sem as permissões de administrador.

Na caixa de diálogo a seguir, selecione o ISP (Internet Service Provider - Provedor de Serviços da Internet). Para escolher a partir de uma lista de ISPs predefinida operacional em seu país, selecione *País*. Ou então, clique em *Novo* para abrir uma caixa de diálogo

em que você fornecerá os dados do seu ISP. Isso inclui um nome para a conexão de discagem e o ISP, assim como o login e a senha fornecidos pelo seu ISP. Habilite *Sempre Solicitar Senha* para que a senha seja solicitada sempre que você se conectar.

Na última caixa de diálogo, especifique as opções de conexão adicionais:

Discagem sob Demanda
: Se você habilitar a discagem sob demanda, configure, pelo menos, um servidor de nomes.

Modificar DNS quando conectado
: Essa opção é habilitada por padrão, com o efeito de que o endereço do servidor de nomes é atualizado sempre que você se conectar à Internet.

Receber DNS automaticamente
: Se o provedor não transmitir seu servidor de nomes de domínio após a conexão, desabilite essa opção e digite os dados do DNS manualmente.

Modo Estúpido
: Essa opção é habilitada por padrão. Com ela, prompts de entrada enviados pelo servidor do ISP são ignorados para que não interfiram no processo de conexão.

Interface Externa do Firewall* e *Reiniciar Firewall
: A seleção dessas opções habilita o SUSEfirewall2, que protege contra ataques externos enquanto você está conectado à Internet.

Tempo Ocioso (em segundos)
: Com essa opção, especifique um período de inatividade da rede depois do qual o modem se desconectará automaticamente.

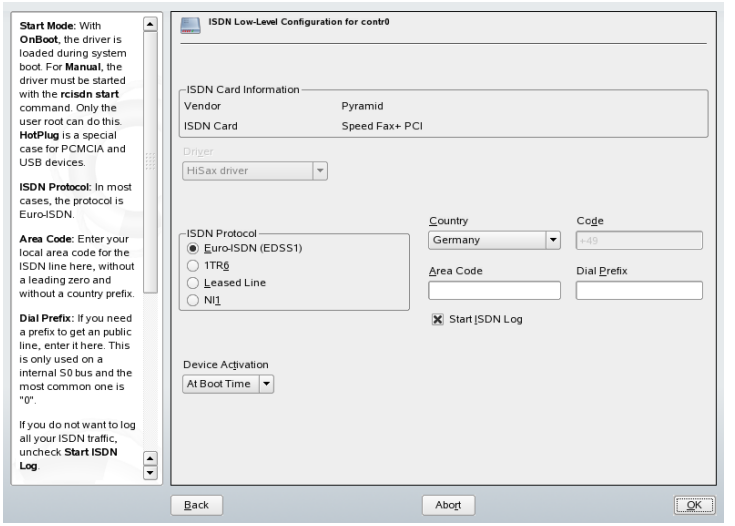
Detalhes IP
: Essa opção abre a caixa de diálogo de configuração de endereço. Se o ISP não designar um endereço IP dinâmico ao host, desabilite *Endereço IP Dinâmico* e, depois, digite o endereço IP local do host e o endereço IP remoto. Peça essa informação ao ISP. Habilite *Rota Padrão* e feche a caixa de diálogo, selecionando *OK*.

Selecionando *Próximo*, você retorna à caixa de diálogo original, que exibirá um resumo da configuração do modem. Feche essa caixa de diálogo com *Concluir*.

38.4.3 ISDN

Use esse módulo para configurar uma ou várias placas ISDN para o seu sistema. Se o YaST não tiver detectado a placa ISDN, selecione-a manualmente. É possível haver várias Interfaces, mas diversos ISPs podem ser configurados para uma única interface. Nas caixas de diálogo subseqüentes, configure as opções de ISDN necessárias para o funcionamento adequado da placa.

Figura 38.5 *Configuração ISDN*

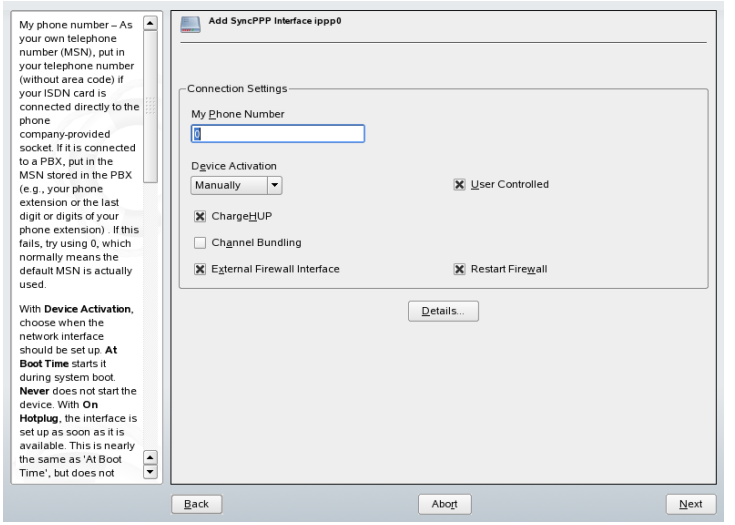

Start Mode: With OnBoot, the driver is loaded during system boot. For Manual, the driver must be started with the rcisdn start command. Only the user root can do this. HotPlug is a special case for PCMCIA and USB devices.
ISDN Protocol: In most cases, the protocol is Euro-ISDN.
Area Code: Enter your local area code for the ISDN line here, without a leading zero and without a country prefix.
Dial Prefix: If you need a prefix to get an public line, enter it here. This is only used on a internal S0 bus and the most common one is "0".
If you do not want to log all your ISDN traffic, uncheck Start ISDN Log.
ISDN Low-Level Configuration for contr0
ISDN Card Information
Vendor
Pyramid
ISDN Card
Speed Fax+ PCI
Driver
HiSax driver
ISDN Protocol
Euro-ISDN (EDSS1)
1TR6
Leased Line
NI1
Country
Germany
Code
+49
Area Code
Dial Prefix
Start ISDN Log
Device Activation
At Boot Time
Back
Abort
OK

Na caixa de diálogo a seguir, mostrada na Figura 38.5, “Configuração ISDN” (p 608), selecione o protocolo a ser usado. O padrão é *Euro-ISDN (EDSS1)*, mas para intercâmbios mais antigos ou maiores, selecione *1TR6*. Se você estiver nos E.U.A., selecione *NI1*. Selecione seu país no campo relevante. O código de país correspondente aparecerá no campo próximo a ele. Por fim, forneça seu *Código de Área* e o *Prefixo de Discagem*, se necessário.

Modo de Início define como a interface do ISDN deve ser iniciada: *Em Tempo de Boot* inicializa o driver do ISDN sempre que o sistema for inicializado. *Manualmente* exige que você carregue o driver do ISDN como `root` com o comando `rcisdn start`. *Em Hotplug*, usado para dispositivos PCMCIA ou USB, carrega o driver depois que o dispositivo é conectado. Ao concluir essas configurações, selecione *OK*.

Na caixa de diálogo a seguir, especifique o tipo de interface para a placa ISDN e adicione ISPs a uma interface existente. As interfaces podem ser do tipo `SyncPPP` ou `RawIP`, mas a maioria dos ISPs opera no modo `SyncPPP`, descrito abaixo.

Figura 38.6 *Configuração da interface ISDN*


My phone number – As your own telephone number (MSN), put in your telephone number (without area code) if your ISDN card is connected directly to the phone company-provided socket. If it is connected to a PBX, put in the MSN stored in the PBX (e.g., your phone extension or the last digit or digits of your phone extension). If this fails, try using 0, which normally means the default MSN is actually used.
With Device Activation, choose when the network interface should be set up. At Boot Time starts it during system boot. Never does not start the device. With On Hotplug, the interface is set up as soon as it is available. This is nearly the same as 'At Boot Time', but does not
Add SyncPPP Interface ippp0
Connection Settings
My Phone Number
0
Device Activation
Manually
User Controlled
ChargeHUP
Channel Bundling
External Firewall Interface
Restart Firewall
Details...
Back
Abort
Next

O número a ser digitado para *Meu Número Telefônico* dependerá da sua configuração específica:

Placa ISDN conectada diretamente à saída do fone

Uma linha ISDN padrão fornece três números telefônicos (chamados MSNs ou multiple subscriber numbers). Se o assinante pediu mais números, poderá ter até 10. Um desses MSNs precisa ser digitado aqui, mas sem o código de área. Se você digitar o número errado, o operador de fone retornará automaticamente ao primeiro MSN designado à sua linha ISDN.

Placa ISDN conectada a um PBX

Novamente, a configuração poderá variar de acordo com o equipamento instalado:

1. PBX menores, criados para fins domésticos, normalmente usam o protocolo Euro-ISDN (EDSS1) para chamadas internas. Esses intercâmbios possuem um barramento S0 interno e usam números internos para o equipamento conectado a eles.

Use um dos números internos como o seu MSN. Você deveria usar, pelo menos, um dos MSNs de intercâmbio habilitados para discagem direta para fora. Se não funcionar, tente um único zero. Para obter mais informações, consulte a documentação que acompanha o intercâmbio do fone.

2. Intercâmbios de fone maiores criados para negócios normalmente usam o protocolo 1TR6 para chamadas internas. Seus MSNs são chamados EAZ e, geralmente, correspondem ao número de discagem direta. Para a configuração no Linux, deverá ser suficiente digitar o último dígito de EAZ. Como última opção, tente cada um dos dígitos de 1 a 9.

Para que a conexão seja encerrada pouco antes de terminar a próxima unidade de carga, habilite *ChargeHUP*. Entretanto, lembre-se de que talvez não funcione com todos os ISPs. Você também pode habilitar o agrupamento de canais (multilink PPP) selecionando a opção correspondente. Por fim, você pode habilitar o SuSEfirewall2 para o link selecionando *Interface Externa do Firewall* e *Reiniciar Firewall*. Para que o usuário normal sem permissões de administrador possa ativar ou desativar a interface, selecione a opção *Controlado pelo Usuário*.

Detalhes abre uma caixa de diálogo em que se implementa esquemas de conexão mais complexos, pouco relevantes para usuários domésticos. Saia da caixa de diálogo *Detalhes* selecionando *OK*.

Na caixa de diálogo seguinte, configure endereços IP. Se o provedor não tiver fornecido um IP estático, selecione *Endereço IP Dinâmico*. Caso contrário, use os campos fornecidos para digitar o endereço IP local e o remoto do seu host, de acordo com as especificações do ISP. Se a interface for a rota padrão para a Internet, selecione *Rota Padrão*. Cada host só pode ter uma interface configurada como a rota padrão. Saia dessa caixa de diálogo selecionando *Próximo*.

A caixa de diálogo a seguir permite que você defina seu país e selecione um ISP. Os ISPs incluídos na lista são apenas provedores do tipo chamada-por-chamada. Se seu ISP não estiver na lista, selecione *Novo*. A caixa de diálogo *Parâmetros do Provedor* será aberta para que você digite todos os detalhes do seu ISP. Ao digitar o número telefônico, não inclua espaços vazios nem vírgulas entre os dígitos. Por fim, digite seu login e senha, conforme fornecido pelo ISP. Ao terminar, selecione *Próximo*.

Para usar *Discagem sob Demanda* em uma estação de trabalho independente, especifique também o servidor de nomes (servidor DNS). A maioria dos ISPs suporta DNS dinâmico, o que significa que o endereço IP de um servidor de nomes é enviado pelo ISP toda

vez que você se conecta. Entretanto, para uma única estação de trabalho, é preciso fornecer um endereço marcador, como `192.168.22.99`. Se o ISP não suportar um DNS dinâmico, especifique os endereços IP do servidor de nomes do ISP. Se desejar, especifique um tempo de espera para a conexão — o período de inatividade da rede (em segundos) depois do qual a conexão deve encerrar automaticamente. Confirme as configurações com *Próximo*. O YaST exibe um resumo das interfaces configuradas. Para ativar todas essas configurações, selecione *Concluir*.

38.4.4 Modem a cabo

Em alguns países, como a Áustria e os E.U.A., é bastante comum acessar a Internet pela rede de TV a cabo. O assinante de TV a cabo normalmente recebe um modem, que é conectado à saída do cabo da TV em uma ponta e à placa de rede do computador na outra (usando um cabo de par trançado 10Base-TG). O modem a cabo então fornece uma conexão dedicada à Internet com um endereço IP fixo.

Dependendo das instruções fornecidas pelo ISP, ao configurar a placa de rede, selecione *Configuração Automática de Endereço (via DHCP)* ou *Configuração de Endereço Estático*. A maioria dos provedores usa atualmente o DHCP. Um endereço IP estático freqüentemente vem como parte de uma conta comercial especial.

38.4.5 DSL

Para configurar o dispositivo DSL, selecione o módulo *DSL* na seção *Dispositivos de Rede* do YaST. O módulo YaST consiste em várias caixas de diálogo nas quais configura-se os parâmetros de links DSL com base em um dos seguintes protocolos:

- PPPoE (PPP sobre Ethernet)
- PPPoATM (PPP sobre ATM)
- CAPI para ADSL (Placas Fritz)
- PPTP (Point-to-Point Tunneling Protocol) — Áustria

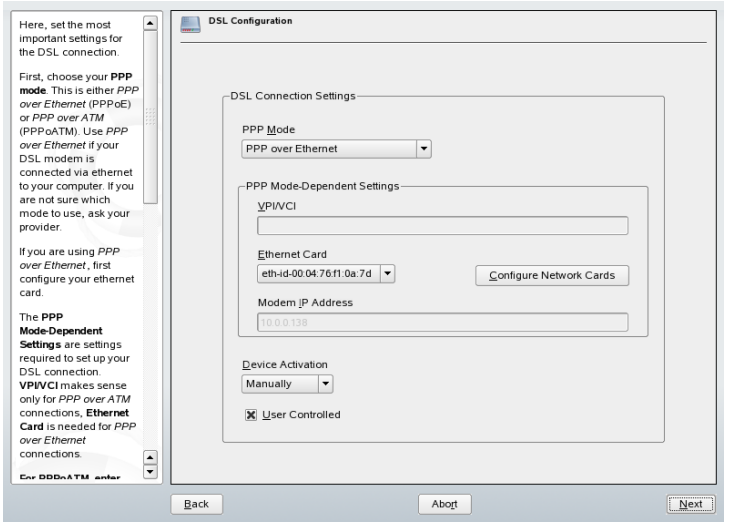
A configuração de uma conexão DSL baseada no PPPoE ou no PPTP exige que a placa de rede correspondente já esteja configurada de forma correta. Se isso ainda não foi feito, primeiro configure a placa, selecionando *Configurar Placas de Rede* (consulte a Seção 38.4.1, “Configurando a placa de rede com o YaST” (p 603)). No caso de um link

DSL, os endereços podem ser designados automaticamente, mas não via DHCP, e é por isso que você não deve habilitar a opção *Configuração Automática de Endereço (via DHCP)*. Em vez disso, digite um endereço estático simulado para a interface, como `192.168.22.1`. Em *Máscara de Sub-rede*, digite `255.255.255.0`. Se estiver configurando uma estação de trabalho independente, deixe a opção *Gateway Padrão* vazia.

DICA

Os valores em *Endereço IP* e *Máscara de Sub-rede* são apenas marcadores. Eles são necessários apenas para inicializar a placa de rede e não representam o link DSL.

Figura 38.7 *Configuração DSL*


Here, set the most important settings for the DSL connection.
First, choose your PPP mode. This is either PPP over Ethernet (PPPoE) or PPP over ATM (PPPoATM). Use PPP over Ethernet if your DSL modem is connected via ethernet to your computer. If you are not sure which mode to use, ask your provider.
If you are using PPP over Ethernet, first configure your ethernet card.
The PPP Mode-Dependent Settings are settings required to set up your DSL connection. VPI/VCI makes sense only for PPP over ATM connections, Ethernet Card is needed for PPP over Ethernet connections.
DSL Configuration
DSL Connection Settings
PPP Mode
PPP over Ethernet
PPP Mode-Dependent Settings
VPI/VCI
Ethernet Card
eth-id-00:04:76:f1:0a:7d
Configure Network Cards
Modem IP Address
10.0.0.138
Device Activation
Manually
User Controlled
Back
Abort
Next

Para iniciar a configuração DSL (consulte a Figura 38.7, "Configuração DSL" (p 612)), primeiro selecione o modo PPP e a placa ethernet à qual o modem DSL está conectado (normalmente, é a `eth0`). Então, use a opção *Ativação do Dispositivo*, para especificar se o link DSL deve ser estabelecido durante o processo de inicialização. Clique em *Controlado pelo Usuário*, para autorizar o usuário normal sem permissões de root para ativar ou desativar a interface com o KInternet. A caixa de diálogo também permite que você selecione seu país e escolha um ISP entre os que nele operam. Os detalhes de quaisquer caixas de diálogo subseqüentes da configuração DSL dependem das opções

configuradas até agora. É por essa razão que eles são apenas rapidamente mencionados nos parágrafos a seguir. Para obter detalhes sobre as opções disponíveis, leia a ajuda detalhada disponível nas caixas de diálogo.

Para usar *Discagem sob Demanda* em uma estação de trabalho independente, especifique também o servidor de nomes (servidor DNS). A maioria dos ISPs suporta DNS dinâmico — o endereço IP de um servidor de nomes é enviado pelo ISP toda vez que você se conecta. Entretanto, para uma única estação de trabalho, é preciso fornecer um endereço marcador, como `192.168.22.99`. Se o ISP não suportar um DNS dinâmico, especifique o endereço IP do servidor de nomes fornecido pelo ISP.

Tempo Ocioso (em segundos) define um período de inatividade da rede depois do qual a conexão é encerrada automaticamente. Um valor de tempo de espera razoável fica entre 60 e 300 segundos. Se a opção *Discagem sob Demanda* estiver desabilitada, talvez seja útil configurar o tempo de espera como zero para evitar um desligamento automático.

A configuração do T-DSL é muito parecida com a do DSL. Basta selecionar *T-Online* como seu provedor e o YaST abrirá a caixa de diálogo de configuração do T-DSL. Nessa caixa de diálogo, forneça algumas informações adicionais necessárias para o T-DSL — o ID da linha, o número do T-Online, o código de usuário e sua senha. Tudo isso deve estar incluído nas informações que você recebeu após se inscrever no T-DSL.

38.5 Configurando uma conexão de rede manualmente

A configuração manual do software de rede deve ser sempre a última alternativa. É recomendável usar o YaST. Entretanto, essas informações de base sobre a configuração de rede também podem ajudar você na utilização do YaST.

Todas as placas de rede embutidas e hotplug (PCMCIA, USB e algumas PCI) são detectadas e configuradas através do hotplug. O sistema identifica uma placa de rede de duas formas diferentes: primeira, como um dispositivo físico e, segunda, como uma interface. A inserção ou detecção de um dispositivo aciona um evento hotplug. Esse evento de hotplug aciona a inicialização do dispositivo com o script `hwup`. Quando a placa de rede é inicializada como uma nova interface de rede, o kernel gera outro evento de hotplug que aciona a configuração da interface com `ifup`.

A interface de números kernel define nomes de acordo com a ordem temporal de seus registros. A seqüência de inicialização é decisiva para a designação de nomes. Se alguma das muitas placas de rede falhar, a numeração de todas as placas inicializadas subseqüentemente será deslocada. Para placas reais que aceitam hotplug, o que importa é a ordem em que os dispositivos são conectados.

Para obter uma configuração flexível, a configuração do dispositivo (hardware) e a interface foram separadas e o mapeamento das configurações para dispositivos e interfaces não é mais gerenciado com base nos nomes de interface. As configurações de dispositivos estão localizadas em `/etc/sysconfig/hardware/hwcfg-*`. As configurações de interface estão localizadas em `/etc/sysconfig/network/ifcfg-*`. Os nomes das configurações são designados de forma que descrevam os dispositivos e as interfaces aos quais estão associados. Como o mapeamento de drivers anterior exigia nomes de interface estáticos, esse tipo de mapeamento não pode mais ocorrer em `/etc/modprobe.conf`. No novo conceito, as entradas de álias desse arquivo causariam efeitos colaterais indesejáveis.

Os nomes de configuração — tudo depois de `hwcfg-` ou `ifcfg-` — podem descrever os dispositivos por meio do slot, um ID específico de dispositivo ou por meio do nome da interface. Por exemplo, o nome de configuração para uma placa PCI poderia ser `bus-pci-0000:02:01.0` (slot PCI) ou `vpid-0x8086-0x1014-0x0549` (ID do produto e fornecedor). O nome da interface associada poderia ser `bus-pci-0000:02:01.0` ou `wlan-id-00:05:4e:42:31:7a` (endereço MAC).

Para designar uma determinada configuração de rede a qualquer placa de determinado tipo (em que apenas uma é inserida de cada vez), em vez de selecionar uma determinada placa, escolha nomes de configuração menos específicos. Por exemplo, `bus-pcmcia` seria usado para todas as placas PCMCIA. Por outro lado, os nomes podem ser limitados por um tipo de interface precedente. Por exemplo, `wlan-bus-usb` seria designado a placas WLAN conectadas a uma porta USB.

O sistema sempre usa a configuração que melhor descreve uma interface ou o dispositivo que a fornece. A pesquisa da configuração mais adequada é executada por `getcfg`. A saída de `getcfg` fornece todas as informações que podem ser usadas para descrever um dispositivo. Detalhes referentes à especificação dos nomes de configuração estão disponíveis na página de manual do `getcfg`.

Com o método descrito, uma interface de rede é configurada corretamente, mesmo que os dispositivos da rede nem sempre sejam inicializados na mesma ordem. Entretanto,

o nome da interface ainda dependerá da seqüência de inicialização. Há duas formas de garantir o acesso confiável à interface de uma determinada placa de rede:

- `getcfg-interface` *`nome da configuração`* retorna o nome da interface de rede associada. Portanto, o nome de configuração, como firewall, dhcpd, roteamento ou várias interfaces de rede virtuais (túneis), pode ser digitado em alguns arquivos de configuração, em vez do nome da interface, que não é persistente.

- Nomes de interface persistentes podem ser designados a todas as interfaces cujas configurações não incluam nomes de interface. Isso pode ser feito por meio de entradas `PERSISTENT_NAME=`*`pname`* em uma configuração de interface (`ifcfg-*`). Entretanto, o nome persistente *`nomep`* não deve ser igual ao que será automaticamente designado pelo kernel. Assim, `eth*`, `tr*`, `wlan*` e assim por diante não são permitidos. Em vez disso, use `net*` ou nomes descritivos, como `externo`, `interno` ou `dmz`. Um nome persistente só pode ser designado a uma interface imediatamente depois de seu registro, o que significa que o driver da placa de rede precisa ser recarregado ou a descrição do dispositivo `hwup` deve ser executada. O comando `rcnetwork restart` não é suficiente para essa finalidade.

IMPORTANTE: Usando nomes de interface persistentes

O uso de nomes de interface persistentes não foi testado em todas as áreas. Portanto, alguns aplicativos talvez não sejam capazes de controlar nomes de interface selecionados livremente.

`ifup` requer uma interface existente, pois não inicializa o hardware. A inicialização do hardware é controlada pelo comando `hwup` (executado por `hotplug` ou `coldplug`). Quando um dispositivo for inicializado, `ifup` será executado automaticamente para a nova interface, através do `hotplug`, e a interface será configurada se o modo de início for `onboot`, `hotplug` ou `auto` e o serviço de `rede` tiver sido iniciado. Anteriormente, o comando `ifup` *`nomedainterface`* acionava a inicialização do hardware. Agora o procedimento foi invertido. Primeiro, o componente de hardware é inicializado e, depois, ocorrem todas as outras ações. Dessa forma, um número variável de dispositivos pode sempre ser configurado da melhor forma possível com um conjunto de configurações existente.

A Tabela 38.5, “Scripts de configuração de rede manual” (p 616) resume os scripts mais importantes envolvidos na configuração de rede. Onde for possível, os scripts são distinguidos pelo hardware e pela interface.

Tabela 38.5 *Scripts de configuração de rede manual*

Estágio da configuração	Comando	Função
Hardware	`hw{up,down,status}`	Os scripts `hw*` são executados por um subsistema hotplug para inicializar um dispositivo, desfazer a inicialização ou consultar o status de um dispositivo. Há mais informações disponíveis na página de manual do `hwup`.
Interface	`getcfg`	`getcfg` pode ser usado para consultar o nome da interface associado a um nome de configuração ou a uma descrição de hardware. Há mais informações disponíveis na página de manual do `getcfg`.
Interface	`if{up,down,status}`	Os scripts `if*` iniciam interfaces de rede existentes ou retornam o status da interface especificada. Há mais informações disponíveis na página do manual de `ifup`.

Há mais informações disponíveis sobre hotplug e nomes de dispositivos persistentes no Capítulo 32, *O sistema hotplug* (p 517) e no Capítulo 33, *Nós de dispositivo dinâmicos com `udev`* (p 525).

38.5.1 Arquivos de configuração

Esta seção fornece uma visão geral dos arquivos de configuração de rede e explica sua finalidade e formato usado.

`/etc/syconfig/hardware/hwcfg-*`

Esses arquivos contêm as configurações de hardware de placas de rede e de outros dispositivos. Eles contêm os parâmetros necessários, como o módulo kernel, modo de

início e associações de script. Consulte a página de manual do `hwup` para obter mais detalhes. Independentemente do hardware existente, as configurações `hwcfg-static-*` são aplicadas quando o coldplug é iniciado.

/etc/sysconfig/network/ifcfg-*

Esses arquivos contêm as configurações da interface de rede. Eles incluem informações, como o modo de início e o endereço IP. Parâmetros possíveis são descritos na página de manual do `ifup`. Além disso, todas as variáveis dos arquivos `dhcp`, `wireless` e `config` podem ser usadas nos arquivos `ifcfg-*` se uma configuração geral for usada somente para uma interface.

/etc/sysconfig/network/config, dhcp, wireless

O arquivo `config` contém configurações gerais para o desempenho de `ifup`, `ifdown` e `ifstatus`. `dhcp` contém configurações para DHCP e `wireless` para placas LAN sem fio. As variáveis em todos os três arquivos de configuração são comentadas e também podem ser usadas nos arquivos `ifcfg-*`, em que são tratadas com prioridade mais alta.

/etc/sysconfig/network/routes,ifroute-*

O roteamento estático dos pacotes TCP/IP é determinado aqui. Todas as rotas estáticas exigidas pelas várias tarefas do sistema podem ser inseridas no arquivo `/etc/sysconfig/network/routes`: rotas para um host, rotas para um host através de um gateway e rotas para uma rede. Para cada interface que necessite de um roteamento individual, defina um arquivo de configuração adicional: `/etc/sysconfig/network/ifroute-*`. Substitua `*` pelo nome da interface. As entradas nos arquivos de configuração de roteamento terão esta aparência:

```
# Destination     Dummy/Gateway     Netmask            Device #
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

O destino da rota está na primeira coluna. Essa coluna pode conter o endereço IP de uma rede ou host ou, no caso de servidores de nomes *acessíveis*, a rede ou o nome de host totalmente qualificado.

A segunda coluna contém o gateway padrão ou um gateway através do qual um host ou uma rede pode ser acessada. A terceira coluna contém a máscara de rede para redes ou hosts atrás de um gateway. Por exemplo, a máscara em `255.255.255.255` para um host atrás de um gateway.

A quarta coluna só é relevante para redes conectadas ao host local, como loopback, Ethernet, ISDN, PPP e dispositivo simulado. O nome do dispositivo deve ser digitado aqui.

Uma quinta coluna (opcional) pode ser usada para especificar o tipo de uma rota. Colunas desnecessárias devem conter um sinal de subtração – para garantir que o analisador interprete o comando corretamente. Para obter mais detalhes, consulte a página de manual das `rotas(5)`.

/etc/resolv.conf

O domínio ao qual o host pertence é especificado neste arquivo (palavra-chave `search`). Também está listado o status do endereço do servidor de nomes para acesso (palavra-chave `nameserver`). Vários nomes de domínios podem ser especificados. Durante a resolução de um nome não totalmente qualificado, uma tentativa de gerar um nome será feita, anexando as entradas de `pesquisa` individuais. Use vários servidores de nomes digitando várias linhas, todas iniciadas pelo `servidor de nomes`. Preceda os comentários com sinais `#`. O YaST insere o servidor de nomes especificado neste arquivo. O Exemplo 38.5, “`/etc/resolv.conf`” (p 618) mostra como a aparência de `/etc/resolv.conf` poderá ser.

Exemplo 38.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as
nameserver nameserver 192.168.0.20
```

Alguns serviços, como `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp` (`dhcpcd` e `dhclient`), `pcmcia` e `hotplug` modificam o arquivo `/etc/resolv.conf` através do script `modify_resolvconf`. Se o arquivo `/etc/resolv.conf` tiver

sido temporariamente modificado por esse script, ele conterá um comentário predefinido com informações sobre o serviço que o modificou, o local onde foi feito o backup do arquivo original e como desligar o mecanismo de modificação automática. Se `/etc/resolv.conf` for modificado várias vezes, o arquivo incluirá modificações de forma aninhada. Isso pode ser revertido de forma completa, mesmo que essa reversão ocorra em uma ordem diferente da ordem em que as modificações foram introduzidas. Entre os serviços que talvez necessitem dessa flexibilidade, estão incluídos `isdn`, `pcmcia` e `hotplug`.

Se um serviço não tiver terminado de forma normal e limpa, `modify_resolvconf` poderá ser usado para restaurar o arquivo original. Da mesma forma, na inicialização do sistema, uma verificação é feita para ver se há um `resolv.conf` modificado que não esteja limpo. Por exemplo, após uma falha no sistema, o `resolv.conf` original (não modificado) será restaurado.

O YaST usa o comando `modify_resolvconf check` para descobrir se o `resolv.conf` foi modificado e, logo depois, avisa o usuário de que as modificações serão perdidas após a restauração do arquivo. Além disso, o YaST não se baseia no `modify_resolvconf`, o que significa que o impacto de modificar o `resolv.conf` através do YaST é o mesmo que o de qualquer mudança manual. Em ambos os casos, as mudanças têm um efeito permanente. As modificações solicitadas pelos serviços mencionados são somente temporárias.

/etc/hosts

Nesse arquivo, mostrado em Exemplo 38.6, “`/etc/hosts`” (p 619), os endereços IP são designados a nomes de host. Se nenhum servidor de nomes for implementado, todos os hosts nos quais uma conexão IP for configurada precisarão ser listados aqui. Para cada host, digite uma linha no arquivo com o endereço IP, o nome de host totalmente qualificado e o nome de host. O endereço IP precisa estar no início da linha e as entradas separadas por espaços vazios e guias. Comentários são sempre precedidos pelo sinal `#`.

Exemplo 38.6 */etc/hosts*

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.0 earth.example.com earth
```

/etc/networks

Aqui, os nomes de rede são convertidos em endereços de rede. O formato é semelhante ao do arquivo `hosts`, exceto que os nomes de rede precedem os endereços. Consulte o Exemplo 38.7, “`/etc/networks`” (p 620).

Exemplo 38.7 *`/etc/networks`*

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

Resolução do nome — a conversão dos nomes de host e de rede através da biblioteca *resolver*— é controlada por esse arquivo. Esse arquivo é usado somente para programas vinculados a libc4 ou libc5. Para programas glibc atuais, consulte as configurações em `/etc/nsswitch.conf`. Um parâmetro precisa estar sempre independente em sua própria linha. Comentários são precedidos pelo sinal `#`. A Tabela 38.6, “Parâmetros para /etc/host.conf” (p 620) mostra os parâmetros disponíveis. Uma amostra de `/etc/host.conf` é mostrada no Exemplo 38.8, “ `/etc/host.conf` ” (p 621).

Tabela 38.6 *Parâmetros para /etc/host.conf*

order *hosts*, *bind*	Especifica em que ordem os serviços são acessados para a resolução de nomes. Os argumentos disponíveis são (separados por espaços vazios ou vírgulas): *hosts*: pesquisa o arquivo `/etc/hosts` *bind*: acessa um servidor de nomes *nis*: usa o NIS
multi *on*/*off*	Define se um host digitado em `/etc/hosts` pode ter vários endereços IP.
nospoof *on* spoofalert *on*/*off*	Esses parâmetros influenciam o *spoofing* do servidor de nomes, mas, além disso, não exercem qualquer influência na configuração da rede.

trim *domainname*	O nome de domínio especificado é separado do nome de host depois da resolução do nome de host (desde que o nome de host inclua o nome de domínio). Essa opção será útil somente se os nomes de um domínio local estiverem no arquivo `/etc/hosts`, mas ainda deverão ser reconhecidos com os nomes de domínio anexados.

Exemplo 38.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow
multiple addrs multi on
```

/etc/nsswitch.conf

O lançamento do GNU C Library 2.0 foi acompanhado pelo lançamento do *NSS* (Name Service Switch). Consulte a página de manual do `nsswitch.conf(5)` e *The GNU C Library Reference Manual* (Manual de Referência da Biblioteca GNU C) para obter mais detalhes.

A ordem das consultas é definida no arquivo `/etc/nsswitch.conf`. Uma amostra do `nsswitch.conf` é exibida em Exemplo 38.9, "/etc/nsswitch.conf" (p 621). Comentários são introduzidos pelo sinal `#`. Neste exemplo, a entrada no banco de dados `hosts` significa que uma solicitação foi enviada para `/etc/hosts` (`arquivos`) através do DNS (consulte oCapítulo 40, *Domain Name System (Sistema de Nomes de Domínio)* (p 633)).

Exemplo 38.9 */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   dns de arquivos

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Os “bancos de dados” disponíveis em NSS estão listados na Tabela 38.7, “Bancos de dados disponíveis através de /etc/nsswitch.conf” (p 622). Além disso, `automount`, `bootparams`, `netmasks` e `publickey` são aguardados em breve. As opções de configuração para bancos de dados NSS estão listadas na Tabela 38.8, “Opções de Configuração para Bancos de Dados “NSS”” (p 623).

Tabela 38.7 *Bancos de dados disponíveis através de /etc/nsswitch.conf*

`aliases`	Álias de correio implementados por `sendmail`; consulte `man 5 aliases`.
`ethers`	Endereços de Ethernet.
`group`	Para grupos de usuários, usados por `getgrent`. Consulte também a página de manual para `group`.
`hosts`	Para nomes de hosts e endereços IP, usados por `gethostbyname` e funções similares.
`netgroup`	Listas de usuários e hosts válidos na rede com a finalidade de controlar permissões de acesso, consulte a página de manual do `netgroup(5)`.
`networks`	Nomes e endereços de redes, usados por `getnetent`.
`passwd`	Senhas de usuários, usadas por `getpwent`; consulte a página de manual do `passwd(5)`.
`protocols`	Protocolos de rede, usados por `getprotoent`; consulte a página de manual do `protocols(5)`.
`rpc`	Nomes e endereços de RPC (Remote Procedure Call) usados por `getrpcbyname` e funções similares.
`services`	Serviços de rede, usados por `getservent`.
`shadow`	Senhas transitórias de usuários, usadas por `getspnam`; consulte a página de manual do `shadow(5)`.

Tabela 38.8 *Opções de Configuração para Bancos de Dados "NSS"*

`arquivos`	arquivos de acesso direto, por exemplo, `/etc/aliases`
`db`	acesso através de um banco de dados
`nis`, `nisplus`	NIS, consulte também o Capítulo 41, *Usando o NIS* (p 655)
`dns`	só pode ser usado como uma extensão de `hosts` e `networks`
`compat`	só pode ser usado como uma extensão de `passwd`, `shadow` e `group`

/etc/nscd.conf

Esse arquivo é usado para configurar o nscd (name service cache daemon). Consulte as páginas de manual de `nscd(8)` e `nscd.conf(5)`. Por padrão, as entradas do sistema de `passwd` e `groups` são armazenadas em cache pelo nscd. Isso é importante para o desempenho de serviços de diretório, como NIS e LDAP, pois, caso contrário, a conexão de rede precisaria ser usada para cada acesso a nomes ou grupos. `hosts` não é armazenado em cache por padrão, porque o mecanismo no nscd para armazenar hosts em cache impede o sistema local de confiar em verificações de pesquisa forward e reverse. Em vez de solicitar ao nscd para armazenar nomes em cache, configure um servidor DNS para armazenamento em cache.

Se o armazenamento em cache de `passwd` estiver ativado, normalmente levará quinze segundos para que um usuário local recentemente adicionado seja reconhecido. Reduza esse tempo de espera reiniciando o nscd com o comando `rcnscd restart`.

/etc/HOSTNAME

Contém o nome de host sem o nome de domínio anexado. Esse arquivo é lido por vários scripts durante a inicialização da máquina. Ele só pode conter uma linha na qual o nome de host é configurado.

38.5.2 Scripts de Inicialização

Além dos arquivos de configuração descritos acima, há também vários scripts que carregam os programas de rede durante a inicialização da máquina. Eles são iniciados assim que o sistema é alternado para um dos *runlevels multiusuário*. Alguns desses scripts são descritos na Tabela 38.9, “Alguns scripts de inicialização para programas de rede” (p 624).

Tabela 38.9 *Alguns scripts de inicialização para programas de rede*

`/etc/init.d/network`	Este script controla a configuração das interfaces de rede. O hardware já precisa ter sido inicializado pelo `/etc/init.d/coldplug` (através do `hotplug`). Se o serviço de `rede` não tiver sido iniciado, nenhuma interface de rede será implementada quando for inserida pelo hotplug.
`/etc/init.d/network`	Inicia o xinetd. O xinetd pode ser usado para disponibilizar os serviços do servidor no sistema. Por exemplo, ele pode iniciar o vsftpd sempre que uma conexão FTP for inicializada.
`/etc/init.d/portmap`	Inicia o portmapper necessário para o servidor RPC, como um servidor NFS.
`/etc/init.d/nfsserver`	Inicia o servidor NFS.
`/etc/init.d/sendmail`	Controla o processo sendmail.
`/etc/init.d/ypserv`	Inicia o servidor NIS.
`/etc/init.d/ypbind`	Inicia o cliente NIS.

38.6 smpppd como Assistente de Discagem

A maioria dos usuários domésticos não possui uma linha dedicada de conexão à Internet. Em vez disso, usam conexões por discagem. Dependendo da forma de discagem (ISDN ou DSL), a conexão é controlada por ipppd ou pppd. Basicamente, tudo que precisa ser feito para estabelecer a conexão é iniciar esses programas corretamente.

Se você tiver uma conexão com tarifa fixa que não gere custos adicionais para a conexão por discagem, basta iniciar o respectivo daemon. Controle a conexão por discagem com um applet KDE ou uma interface de linha de comando. Se o portal de Internet não for o host que você estiver usando, você poderá controlar a conexão por discagem por intermédio de um host de rede.

É aí que entra o smpppd. Ele oferece uma interface uniforme para programas auxiliares e funciona nas duas direções. Primeiro, ele programa o pppd ou ipppd necessário e controla suas propriedades de discagem. Em segundo lugar, disponibiliza diversos provedores aos programas do usuário e transmite informações sobre o atual status da conexão. Já que o smpppd também pode ser controlado por meio da rede, é adequado para controlar conexões por discagem à Internet a partir de uma estação de trabalho de uma sub-rede privada.

38.6.1 Configurando o smpppd

As conexões fornecidas pelo smpppd são automaticamente configuradas pelo YaST. Os programas por discagem KInternet e cinternet propriamente ditos também são pré-configurados. Configurações manuais somente são necessárias para configurar recursos adicionais do smpppd, como o controle remoto.

O arquivo de configuração do smpppd é o `/etc/smpppd.conf`. Por padrão, ele não habilita o controle remoto. As opções mais importantes desse arquivo de configuração são:

open-inet-socket = *yes|no*
: Para controlar o smpppd por meio da rede, essa opção precisa ser definida como `yes`. A porta em que o smpppd realiza a escuta é a `3185`. Se esse parâmetro for

definido como `yes`, os parâmetros `bind-address`, `host-range` e `password` deverão ser definidos da mesma forma.

bind-address = *ip*
Se um host tiver diversos endereços IP, use esse parâmetro para determinar o endereço IP em que o smpppd deve aceitar conexões.

host-range = *min ip max ip*
O parâmetro `host-range` define uma faixa de rede. Os hosts cujos endereços IP se situam dentro dessa faixa recebem acesso ao smpppd. O acesso é recusado a todos os hosts localizados fora dessa faixa.

password = *senha*
Ao atribuir uma senha, limite os clientes a hosts autorizados. Como se trata de uma senha de texto simples, não é recomendável superestimar a segurança por oferecida. Se nenhuma senha for atribuída, todos os clientes terão permissão para acessar o smpppd.

slp-register = *yes|no*
Com esse parâmetro, o serviço smpppd pode ser anunciado na rede por meio do SLP.

Mais informações sobre o smpppd estão disponíveis nas páginas do manual `smpppd(8)` e `smpppd.conf(5)`.

38.6.2 Configurando KInternet, cinternet e qinternet para Uso Remoto

KInternet, cinternet e qinternet podem ser usados para controlar um smpppd local ou remoto. O cinternet é o equivalente da linha de comando do KInternet gráfico. Em linhas gerais, como o qinternet é idêntico ao KInternet, mas não usa as bibliotecas do KDE, pode ser usado sem o KDE e deve ser instalado separadamente. Para preparar esses utilitários para uso com um smpppd remoto, edite o arquivo de configuração `/etc/smpppd-c.conf` manualmente ou com o KInternet. Esse arquivo usa três opções apenas:

sites = *lista de sites*
Indique aos front ends onde procurar o smpppd. Os front ends testam as opções na ordem especificada. A opção `local` ordena o estabelecimento de uma conexão ao

smpppd local. O `gateway` aponta para um smpppd no gateway. A conexão deve ser estabelecida conforme especificações contidas em `server`, em `config-file`. O `slp` ordena aos front ends que se conectem a um smpppd encontrado por meio do SLP.

server = *`servidor`*
Especifique o host em que o smpppd deve ser executado.

password = *`senha`*
Insira a senha selecionada para o smpppd.

Se o smpppd estiver ativo, será possível acessá-lo, por exemplo, com `cinternet --verbose --interface-list`. Se você tiver dificuldades nesse ponto, consulte as páginas do manual `smpppd-c.conf(5)` e `cinternet(8)`.

39 Serviços SLP na rede

O *SLP* foi criado para simplificar a configuração dos clientes em rede dentro de uma rede local. Para configurar um cliente em rede, inclusive todos os serviços necessários, o administrador normalmente precisa ter conhecimento detalhado dos servidores disponíveis na rede. O SLP divulga a disponibilidade de um determinado serviço a todos os clientes da rede local. Os aplicativos que dão suporte ao SLP podem usar as informações distribuídas e podem ser configurados automaticamente.

O SUSE Linux dá suporte à instalação com o uso de origens de instalação fornecidas via SLP e contém diversos serviços de sistema com suporte integrado para SLP. O YaST e o Konqueror possuem front ends apropriados para SLP. Você pode usar o SLP para oferecer funções centrais aos clientes em rede, como um servidor de instalação, servidor YOU, servidor de arquivos ou servidor de impressão no SUSE Linux.

39.1 Registrando seus próprios serviços

Muitos aplicativos contidos no SUSE Linux já possuem suporte integrado ao SLP com o uso da biblioteca `libslp`. Se um serviço não tiver sido compilado com o suporte ao SLP, use um dos métodos a seguir para disponibilizá-lo com SLP:

Registro estático via `/etc/slp.reg.d`
Crie um arquivo de registro separado para cada novo serviço. A seguir há um exemplo de arquivo para o registro de serviço de scanner:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

A linha mais importante desse arquivo é a linha *URL do serviço*, que começa com `service:`. Essa linha contém o tipo de serviço (`scanner.sane`) e o endereço em que o serviço está disponível no servidor. *`$HOSTNAME`* é automaticamente substituída pelo nome completo do host. Em seguida, vem o nome da porta TCP em que o serviço em questão pode ser encontrado, separado por dois-pontos. A seguir, especifique o idioma em que o serviço deve ser exibido e a duração do registro em segundos. Esses dados devem ser separados do URL do serviço por vírgulas. Defina o valor da duração do registro entre `0` e `65535`. O valor `0` impede o registro. O valor `65535` elimina todas as restrições.

O arquivo de registro também contém as duas variáveis `watch-tcp-port` e `descriç o`. A primeira associa o anúncio do serviço SLP à atividade do serviço em questão fazendo com que o slpd verifique o status do serviço. A segunda variável contém uma descrição mais precisa do serviço que é exibido nos browsers aplicáveis.

Registro estático com `/etc/slp.reg`
A única diferença em relação ao procedimento anterior é o agrupamento de todos os serviços em um arquivo central.

Registro dinâmico com slptool
Se um serviço tiver de ser registrado para o SLP a partir de scripts proprietários, use o front end de linha de comando slptool.

39.2 Front ends de SLP no SUSE Linux

O SUSE Linux contém diversos front ends que permitem que as informações relativas ao SLP sejam verificadas e usadas por meio de uma rede:

slptool
O slptool é um programa de linha de comando simples que pode ser usado para anunciar consultas SLP na rede ou anunciar serviços proprietários. `slptool --help` relaciona todas as opções e funções disponíveis. O slptool também pode ser chamado a partir de scripts que processam informações relativas ao SLP.

Browser SLP do YaST
O YaST contém um browser SLP separado que lista todos os serviços da rede local anunciados via SLP em um diagrama em forma de árvore em *Serviços de Rede → Browser SLP*.

Konqueror
Quando usado como um browser de rede, o Konqueror pode exibir todos os serviços SLP disponíveis na rede local em `slp:/`. Clique nos ícones da janela principal para obter mais informações detalhadas sobre o serviço em questão. Se você usar o Konqueror com `service:/`, clique no respectivo ícone uma vez na janela do browser para configurar uma conexão com o serviço selecionado.

39.3 Ativando o SLP

O slpd deve ser executado no seu sistema se você desejar oferecer serviços. Não é necessário iniciar esse daemon apenas para fazer consultas sobre serviços. Assim como a maioria dos serviços de sistema no SUSE Linux, o daemon slpd é controlado por intermédio de um script de inicialização separado. O daemon fica inativo por padrão. Para ativá-lo durante uma sessão, execute `rcslpd start` como `root` para iniciá-lo e `rcslpd stop` para interrompê-lo. Efetue uma verificação de reinicialização ou status com `restart` ou `status`. Se o slpd tiver de ficar ativo por padrão, execute o comando `insserv slpd` uma vez como `root`. Essa ação inclui automaticamente o slpd no conjunto de serviços a serem iniciados durante a inicialização de um sistema.

39.4 Mais informações

As fontes a seguir fornecem informações adicionais sobre o SLP:

RFC 2608, 2609, 2610
O RFC 2608 geralmente trata da definição de SLP. O RFC 2609 trata da sintaxe dos URLs de serviço usados em maior detalhe e o RFC 2610 trata do DHCP via SLP.

http://www.openslp.com
A home page do projeto OpenSLP.

file:/usr/share/doc/packages/openslp/*
Esse diretório contém toda a documentação disponível sobre SLP, inclusive um arquivo `README.SuSE` contendo os detalhes sobre o SUSE Linux, os RFCs citados acima e dois documentos HTML introdutórios. Os programadores que desejarem usar as funções SLP devem instalar o pacote `openslp-devel` para consultar o *Programmers Guide* (Guia de Programadores) que o acompanha.

Domain Name System (Sistema de Nomes de Domínio) 40

O DNS (Domain Name System - Sistema de Nomes de Domínio) é necessário para resolver nomes de domínio e nomes de host em endereços IP. Dessa forma, o endereço IP 192.168.0.0 é designado ao nome de host `earth`, por exemplo. Antes de configurar o servidor de nomes, leia as informações gerais sobre o DNS na Seção 38.3, “Resolução de nomes” (p 601). Os exemplos de configuração a seguir se referem ao BIND.

40.1 Informações básicas sobre o DNS

40.2 Configuração com o YaST

Você pode usar o módulo DNS do YaST para configurar um servidor DNS em sua rede local. Quando o módulo é iniciado pela primeira vez, um assistente é iniciado, solicitando que você tome algumas decisões básicas com relação à administração do servidor. A conclusão desse procedimento inicial propicia uma configuração básica do servidor, que deve funcionar nos aspectos essenciais. O modo de especialista pode ser usado para lidar com tarefas de configuração mais avançadas.

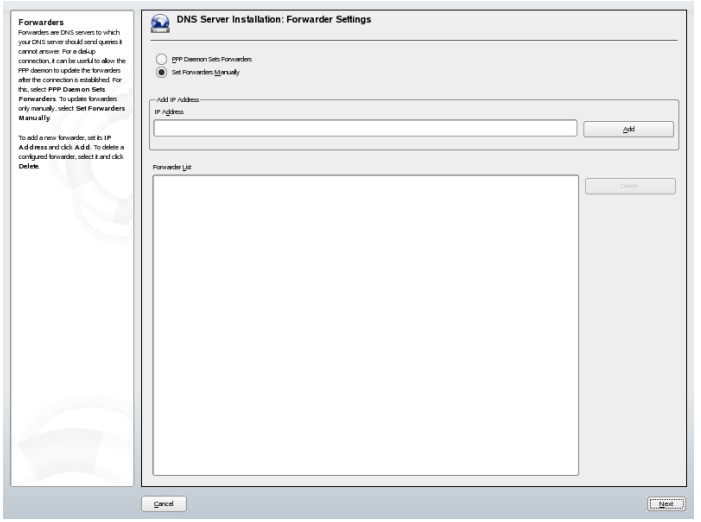
40.2.1 Configuração do assistente

O assistente consiste em três etapas ou caixas de diálogo. Nos locais apropriados das caixas de diálogo, você terá a oportunidade de inserir o modo de configuração de especialista.

Configurações do encaminhador

Ao iniciar o módulo pela primeira vez, consulte a caixa de diálogo exibida na Figura 40.1, “Instalação do servidor DNS: configurações do encaminhador” (p 634). Decida se o daemon PPP deve fornecer uma lista de encaminhadores de chamada via DSL ou ISDN (*O Daemon PPP Define os Encaminhadores*) ou se você deseja fornecer a própria lista (*Definir Encaminhadores Manualmente*).

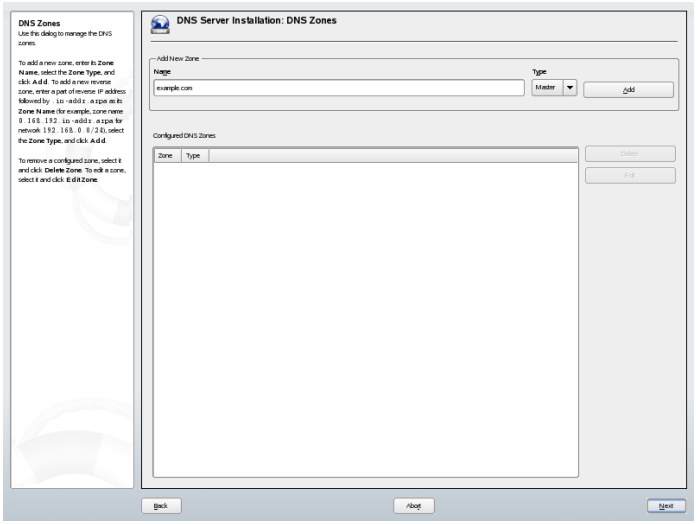
Figura 40.1 *Instalação do servidor DNS: configurações do encaminhador*



Zonas do DNS

Esta caixa de diálogo consiste em várias partes e é responsável pelo gerenciamento de arquivos da zona, descrito na Seção 40.5, “Arquivos de zona” (p 648). Forneça um nome para uma nova zona em *Nome da Zona*. Para adicionar uma zona reversa, o nome deve terminar em `.in-addr.arpa`. Finalmente, selecione o *Tipo de Zona* (master ou escrava). Consulte a Figura 40.2, “Instalação do servidor DNS: zonas do DNS” (p 635). Clique em *Editar Zona* para definir outras configurações em uma zona existente. Para remover uma zona, clique em *Apagar Zona*.

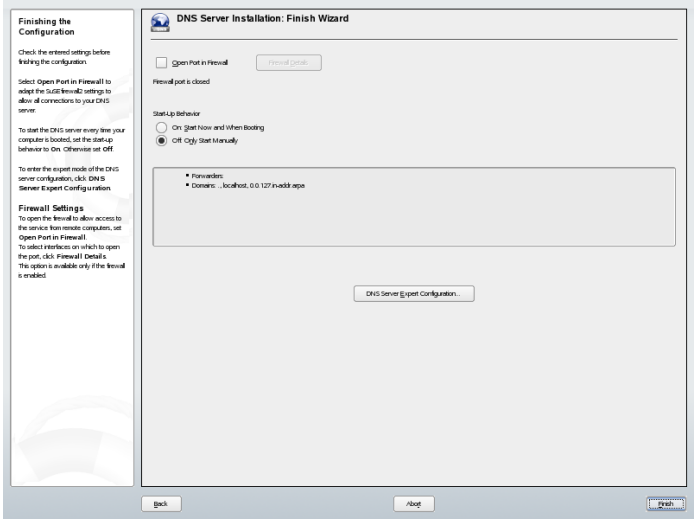
Figura 40.2 *Instalação do servidor DNS: zonas do DNS*


DNS Zones
Use this dialog to manage the DNS zones.
To add a new zone, enter its Zone Name, select the Zone Type, and click Add. To add a new reverse zone, enter a part of reverse IP address followed by .in-addr.arpa as its Zone Name (for example, zone name 0.168.192.in-addr.arpa for network 192.168.0.0/24), select the Zone Type, and click Add.
To remove a configured zone, select it and click Delete Zone. To edit a zone, select it and click Edit Zone.
DNS Server Installation: DNS Zones
Add New Zone
Name
Type
example.com
Master
Add
Configured DNS Zones
Zone
Type
Delete
Edit
Back
Abort
Next

Finalizar Assistente

Na caixa de diálogo final, é possível abrir as portas do serviço DNS no firewall ativado durante a instalação e decidir se o DNS deve ser iniciado. A configuração de especialista também pode ser acessada nessa caixa de diálogo. Consulte a Figura 40.3, “Instalação do servidor DNS: Finalizar Assistente” (p 636).

Figura 40.3 *Instalação do servidor DNS: Finalizar Assistente*


Finishing the Configuration
Check the entered settings before finishing the configuration.
Select Open Port in Firewall to adapt the SuSEfirewall2 settings to allow all connections to your DNS server.
To start the DNS server every time your computer is booted, set the start-up behavior to On. Otherwise set Off.
To enter the expert mode of the DNS server configuration, click DNS Server Expert Configuration.
Firewall Settings
To open the firewall to allow access to the service from remote computers, set Open Port in Firewall.
To select interfaces on which to open the port, click Firewall Details.
This option is available only if the firewall is enabled.
DNS Server Installation: Finish Wizard
Open Port in Firewall
Firewall Details...
Firewall port is closed
Start-Up Behavior
On Start Now and When Booting
Off Only Start Manually
Forwarders:
Domains: ., localhost, 0.0.127.in-addr.arpa
DNS Server Expert Configuration...
Back
Abort
Finish

40.2.2 Configuração de especialista

Depois de iniciar o módulo, o YaST abre uma janela exibindo várias opções de configuração. A definição dessas opções resulta em uma configuração de servidor DNS com as funções básicas estabelecidas:

Inicializar
: Em *Inicializar*, defina se o servidor DNS deve ser inicializado juntamente com a inicialização do sistema ou manualmente. Para iniciar o servidor DNS imediatamente, selecione *Iniciar Servidor DNS Agora*. Para encerrar o servidor DNS, selecione *Parar Servidor DNS Agora*. Para gravar as configurações atuais, selecione *Salvar Configurações e Reiniciar Servidor DNS Agora*. É possível abrir a porta do DNS no firewall com a opção *Abrir Porta no Firewall* e modificar as configurações do firewall com *Detalhes do Firewall*.

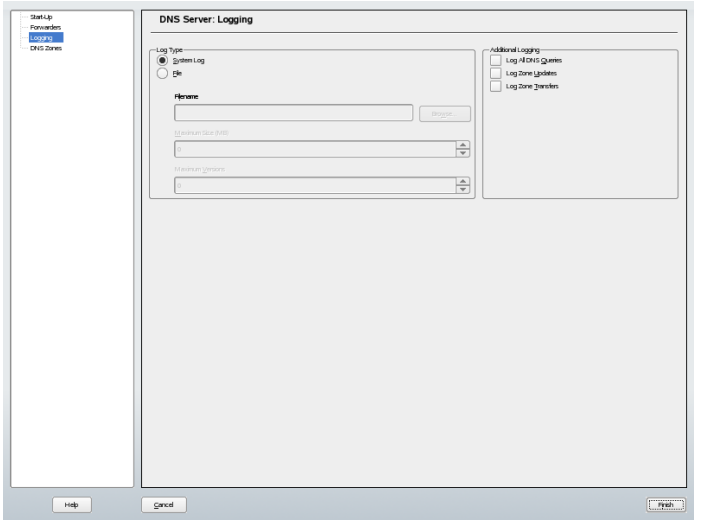
Encaminhadores
: Esta é a mesma caixa de diálogo que foi aberta depois do início da configuração do assistente (consulte Configurações do encaminhador (p 634)).

Registro

Esta seção permite definir o que o servidor DNS deve registrar e como. Em *Tipo de Log*, especifique o local em que o servidor DNS deve gravar os dados de registro. Use o arquivo de registro `/var/log/messages` de todo o sistema selecionando *Inserir no Registro do Sistema*, ou especifique um arquivo diferente selecionando *Registrar em Arquivo*. Nesse caso, especifique também o tamanho máximo do arquivo em megabytes e o número de arquivos de registro a serem armazenados.

Outras opções estão disponíveis em *Registro Adicional*. A habilitação do recurso *Registrar Todas as Consultas de DNS* faz com que *todas* as consultas sejam registradas, caso em que o arquivo de registro pode ficar extremamente grande. Por essa razão, não é uma boa idéia habilitar essa opção para fins que não sejam de depuração. Para registrar o tráfego de dados durante as atualizações de zonas entre o DHCP e o servidor DNS, habilite a opção *Registrar Atualizações de Zona*. Para registrar o tráfego de dados durante uma transferência de zona de master para escrava, habilite a opção *Registrar Transferência de Zonas*. Consulte a Figura 40.4, “Servidor DNS: registro” (p 637).

Figura 40.4 *Servidor DNS: registro*



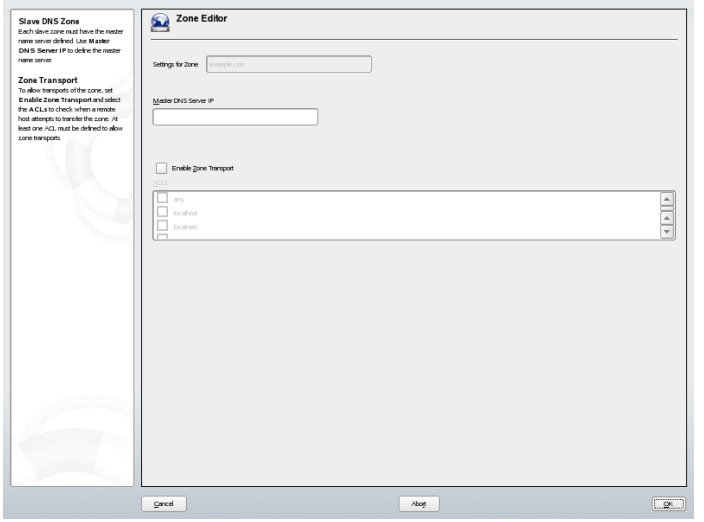
Zonas do DNS

Esta caixa de diálogo é explicada para a configuração do assistente. Consulte a Seção 40.2.1, “Configuração do assistente” (p 634).

Editor de Zona Escrava

Esta caixa de diálogo será aberta se você selecionar o tipo de zona *Escrava* na etapa descrita em Zonas do DNS (p 637). Em *Servidor DNS Master*, especifique o master no qual a escrava deve buscar seus dados. Para limitar acesso ao servidor, selecione um dos ACLs da lista. Consulte a Figura 40.5, "Servidor DNS: Editor de Zona Escrava" (p 638).

Figura 40.5 *Servidor DNS: Editor de Zona Escrava*


Slave DNS Zone
Each slave zone must have the master name server defined. Use Master DNS Server IP to define the master name server.
Zone Transport
To allow transports of the zone, set Enable Zone Transport and select the ACLs to check when a remote host attempts to transfer the zone. At least one ACL must be defined to allow zone transports.
Zone Editor
Settings for Zone
example.com
Master DNS Server IP
Enable Zone Transport
ACLs
any
localhost
localnets
Cancel
About
OK

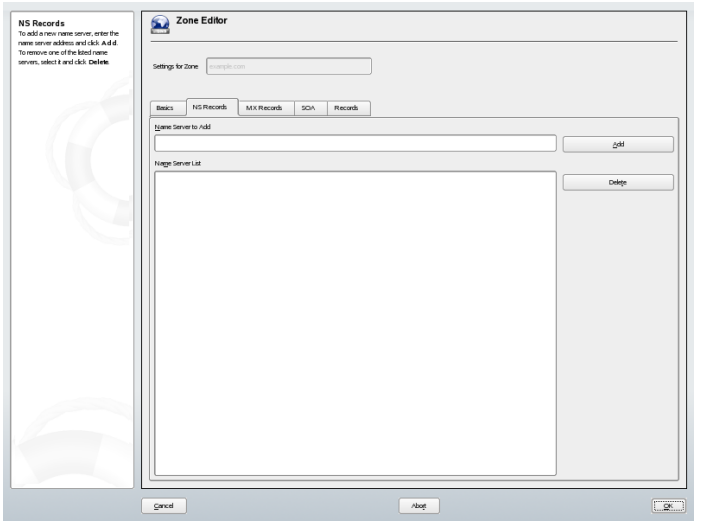
Editor de Zona Master

Esta caixa de diálogo será aberta se você selecionar o tipo de zona *Master* na etapa descrita em Zonas do DNS (p 637). A caixa de diálogo compreende várias páginas: *Básico* (a aberta primeiro), *Registros NS*, *Registros MX*, *SOA* e *Registros*.

Editor de Zona (Registros NS)

Esta caixa de diálogo permite definir servidores de nomes alternativos nas zonas especificadas. Verifique se o nome do seu próprio servidor está incluído na lista. Para adicionar um registro, digite o nome dele em *Servidor de Nome para Adicionar* e, em seguida, confirme com *Adicionar*. Consulte a Figura 40.6, "Servidor DNS: Editor de Zona (Registros NS)" (p 639).

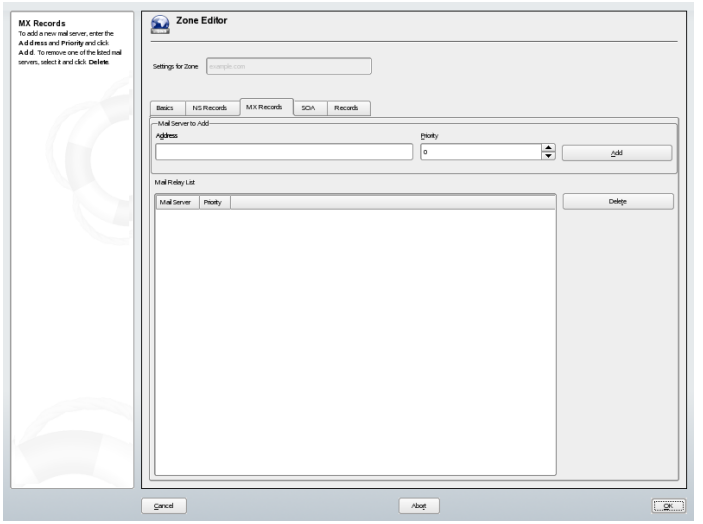
Figura 40.6 *Servidor DNS: Editor de Zona (Registros NS)*



Editor de Zona (Registros MX)

Para adicionar á lista existente um servidor de correio eletrônico para a zona atual, digite o endereço correspondente e o valor de prioridade. Depois disso, confirme a seleção em *Adicionar*. Consulte a Figura 40.7, “Servidor DNS: Editor de Zona (Registros MX)” (p 640).

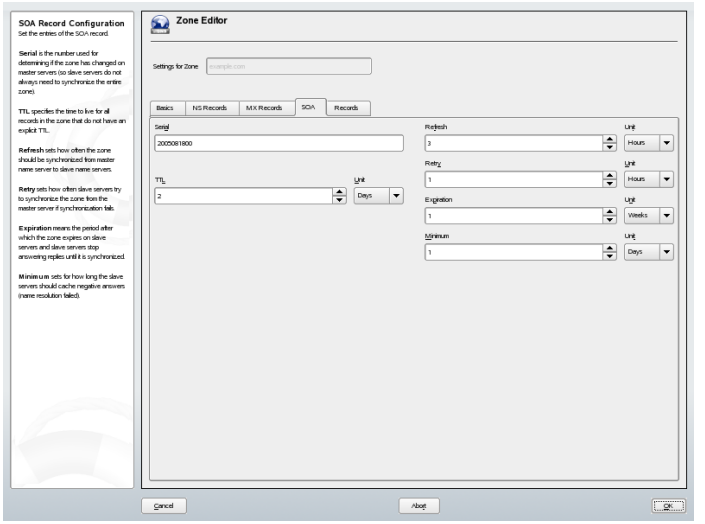
Figura 40.7 *Servidor DNS: Editor de Zona (Registros MX)*



Editor de Zona (SOA)

Esta página permite criar registros de SOA (start of authority). Para obter uma explicação sobre opções específicas, consulte o Exemplo 40.6, “Arquivo /var/lib/named/world.zone” (p 648).

Figura 40.8 *Servidor DNS: Editor de Zona (SOA)*


SOA Record Configuration
Set the entries of the SOA record.
Serial is the number used for determining if the zone has changed on master servers (so slave servers do not always need to synchronize the entire zone).
TTL specifies the time to live for all records in the zone that do not have an explicit TTL.
Refresh sets how often the zone should be synchronized from master name server to slave name servers.
Retry sets how often slave servers try to synchronize the zone from the master server if synchronization fails.
Expiration means the period after which the zone expires on slave servers and slave servers stop answering replies until it is synchronized.
Minimum sets for how long the slave servers should cache negative answers (name resolution failed).
Zone Editor
Settings for Zone
Basics
NS Records
MX Records
SOA
Records
Serial
2005081800
Refresh
3
Unit
Hours
Retry
1
Unit
Hours
TTL
2
Unit
Days
Expiration
1
Unit
Weeks
Minimum
1
Unit
Days
Cancel
Abort
OK

Editor de Zona (Registros)

Esta caixa de diálogo gerencia a resolução de nomes. Em *Chave de Registro*, digite o nome de host e selecione seu tipo. *A-Record* representa a entrada principal. Seu valor deve ser um endereço IP. *CNAME* é um álias. Utilize os tipos *NS* e *MX* para obter registros detalhados ou parciais que expandam as informações fornecidas nas guias *Registros NS* e *Registros MX*. Estes três tipos resolvem um registro A existente. *PTR* é para zonas reversas. É o oposto de um registro A.

40.3 Iniciando o BIND do servidor de nomes

Em um sistema SUSE Linux, o BIND (*Berkeley Internet Name Domain - Domínio de Nomes Berkeley da Internet*) do servidor de nomes vem pré-configurado, de forma que ele pode ser iniciado logo após a instalação, sem problemas. Se você já tiver uma conexão de Internet em funcionamento e digitar `127.0.0.1` como endereço do servidor de nomes para `localhost`, em `/etc/resolv.conf`, já terá uma resolução de nomes em funcionamento, sem que seja necessário conhecer o DNS do provedor. O BIND realiza a resolução de nomes por meio do servidor de nomes raiz, um processo notavelmente mais lento. Normalmente, o DNS do provedor deve ser digitado com o

endereço IP no arquivo de configuração `/etc/named.conf`, em `forwarders`, para garantir uma resolução de nomes segura e eficaz. Se ele estiver funcionando até agora, o servidor de nomes será executado como um servidor de nomes *apenas para cache*. Somente quando você configurar as zonas dele próprio, ele se tornará um DNS adequado. Um exemplo simples disso está incluído na documentação, em `/usr/share/doc/packages/bind/sample-config`.

DICA: Adaptação automática das informações do servidor de nomes

Dependendo do tipo de conexão de Internet ou de conexão de rede, as informações do servidor de nomes podem ser automaticamente adaptadas às condições atuais. Para isso, defina a variável `MODIFY_NAMED_CONF_DYNAMICALLY` no arquivo `/etc/sysconfig/network/config` como `yes`.

Entretanto, não configure nenhum domínio oficial antes de algum ser designado pela instituição responsável. Mesmo que você tenha seu próprio domínio e ele seja gerenciado pelo provedor, é melhor não utilizá-lo, pois o BIND não encaminharia solicitações para esse domínio. O servidor Web no provedor, por exemplo, poderia não ficar acessível para esse domínio.

Para iniciar o servidor de nomes, digite o comando `rcnamed start` como `root`. Se "done" for exibido à direita, em verde, e com o mesmo nome do processo do servidor de nomes, esse servidor terá sido iniciado com êxito. Teste o servidor de nomes imediatamente no sistema local com os programas `host` ou `dig`, que devem retornar `localhost` como servidor padrão, com o endereço `127.0.0.1`. Se esse não é o caso, o arquivo `/etc/resolv.conf` provavelmente contém uma entrada de servidor de nomes incorreta ou não existe. No primeiro teste, digite `host 127.0.0.1`, que sempre funciona. Se você obtiver uma mensagem de erro, use `rcnamed status` para verificar se o servidor está sendo realmente executado. Se o servidor de nomes não for iniciado ou agir de forma inesperada, você poderá encontrar a causa no arquivo de registro `/var/log/messages`.

Para usar o servidor de nomes do provedor ou um servidor de nomes que já esteja em execução na rede como encaminhador, digite o endereço IP ou os endereços correspondentes na seção `options`, em `forwarders`. Os endereços incluídos no Exemplo 40.1, "Opções de encaminhamento no named.conf" (p 643) são apenas exemplos. Ajuste essas entradas de acordo com sua própria configuração.

Exemplo 40.1 *Opções de encaminhamento no named.conf*

```
options {
 directory "/var/lib/named";
 forwarders { 10.11.12.13; 10.11.12.14; };
 listen-on { 127.0.0.1; 192.168.0.99; };
 allow-query { 127/8; 192.168.0/24; };
 notify no;
 };
```

A entrada `options` é seguida de entradas para a zona, `localhost` e `0.0.127.in-addr.arpa`. A entrada `type hint` em "." deve estar sempre presente. Os arquivos correspondentes não precisam ser modificados e devem funcionar como estão. Verifique também se cada entrada está fechada com um ";" e se as chaves estão nos locais corretos. Depois de mudar o arquivo de configuração `/etc/named.conf` ou os arquivos de zona, solicite ao BIND que os releia com o comando `rcnamed reload`. Faça o mesmo interrompendo e reiniciando o servidor de nomes com `rcnamed restart`. Pare o servidor a qualquer momento digitando `rcnamed stop`.

40.4 O arquivo de configuração /etc/named.conf

Todas as configurações do servidor de nomes BIND são armazenadas no arquivo `/etc/named.conf`. Entretanto, os dados de zona que os domínios devem gerenciar, consistindo em nomes de host, endereços IP etc, são armazenados em arquivos separados, no diretório `/var/lib/named`. Os detalhes serão descritos posteriormente.

`/etc/named.conf` é dividido em aproximadamente duas áreas. Uma é a seção `options` para configurações gerais, e a outra consiste nas entradas da `zone` dos domínios específicos. Uma seção `logging` e entradas de `acl` (access control list - lista de controles de acesso) são opcionais. Linhas de comentário começam com um sinal de # ou `//`. Um arquivo `/etc/named.conf` mínimo é exibido no Exemplo 40.2, "Um arquivo /etc/named.conf básico" (p 644).

Exemplo 40.2 *Um arquivo /etc/named.conf básico*

```
options {
 directory "/var/lib/named";
    forwarders { 10.0.0.1; };
 notify no;
};

zone "localhost" in {
 type master;
 file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
 type master;
 file "127.0.0.zone";
};

zone "." in {
 type hint;
 file "root.hint";
};
```

40.4.1 Opções importantes de configuração

diretório "*nomedoarquivo*";
Especifica o diretório no qual o BIND pode encontrar os arquivos contendo os dados da zona. Normalmente, é o `/var/lib/named`.

forwarders { *endereço-ip*; };
Especifica os servidores de nomes (principalmente do provedor) para os quais as solicitações do DNS devem ser encaminhadas se não puderem ser resolvidas diretamente. Substitua *endereço-ip* por um endereço IP como `10.0.0.1`.

forward first;
Faz com que solicitações do DNS sejam encaminhadas antes de uma tentativa ser feita para resolvê-las por meio dos servidores de nomes raiz. Em vez de `forward first`, é possível escrever `forward only` para que todas as solicitações sejam encaminhadas e nenhuma delas seja enviada para os servidores de nomes raiz. Isso faz sentido para configurações de firewall.

listen-on port 53 { 127.0.0.1; *endereço-ip*; };

Comunique ao BIND em que interfaces de rede e porta ele deve aceitar consultas de cliente. A `porta 53` não precisa ser especificada explicitamente, pois `53` é a porta padrão. Digite `127.0.0.1` para permitir solicitações do host local. Se você omitir totalmente essa entrada, todas as interfaces serão usadas por padrão.

listen-on-v6 port 53 {any; };

Comunique ao BIND qual porta ele deve escutar para solicitações de clientes IPv6. A única alternativa para `any` é `none`. Até onde o IPv6 está envolvido, o servidor só aceita um endereço curinga.

query-source address * port 53;

Esta entrada será necessária se um firewall estiver bloqueando as solicitações de saída do DNS. Assim o BIND é avisado para publicar as solicitações externamente à porta 53, e não de qualquer outra porta superior acima da 1024.

query-source-v6 address * port 53;

Comunica ao BIND qual porta deve ser usada para consultas do IPv6.

allow-query { 127.0.0.1; *rede*; };

Define as redes a partir das quais os clientes podem publicar solicitações de DNS. Substitua *`rede`* pelas informações de endereço, como `192.168.1/24`. `/24`, no fim, é uma expressão de abreviação para uma máscara de rede, neste caso, `255.255.255.0`.

allow-transfer ! *;;

controla quais hosts podem solicitar transferências de zona. No exemplo, tais solicitações são completamente negadas com `! *`. Sem essa entrada, as transferências de zona podem ser solicitadas de qualquer local, sem restrições.

statistics-interval 0;

Na ausência desta entrada, o BIND gera várias linhas de informações estatísticas por hora em `/var/log/messages`. Defina-a como 0 para suprimir totalmente estas estatísticas ou definir um intervalo em minutos.

cleaning-interval 720;

Esta opção define os intervalos de tempo em que o BIND limpa seu cache. Ela aciona uma entrada em `/var/log/messages` sempre que isso ocorre. A especificação de tempo é em minutos. O padrão é de 60 minutos

interface-interval 0;
O BIND pesquisa regularmente as interfaces de rede em busca de interfaces novas ou não existentes. Se seu valor for definido como `0`, isso não será feito, e o BIND escutará apenas as interfaces detectadas na inicialização. Caso contrário, o intervalo poderá ser definido em minutos. O padrão é de 60 minutos

notify no;
`no` evita que outros servidores de nomes sejam informados sobre a ocorrência de mudanças nos dados da zona ou sobre quando o servidor de nomes foi reiniciado.

40.4.2 Registro

O BIND pode ser extensivamente configurado para que se determine qual registro está sendo usado, como e onde. Normalmente, as configurações padrão devem ser suficientes. O Exemplo 40.3, “Entrada para desabilitar o registro” (p 646) mostra a forma mais simples de uma entrada como esta e suprime totalmente qualquer registro.

Exemplo 40.3 *Entrada para desabilitar o registro*

```
logging {
 category default { null; };
};
```

40.4.3 Entradas das zonas

Exemplo 40.4 *Entrada da zona para my-domain.de*

```
zone "my-domain.de" in {
 type master;
 file "my-domain.zone";
 notify no;
};
```

Depois de `zone`, especifique o nome do domínio para o administrador (`my-domain.de`), seguido de `in` e um bloco de opções relevantes incluídas entre chaves, como mostrado no Exemplo 40.4, “Entrada da zona para my-domain.de” (p 646). Para definir uma *zona escrava*, altere `type` para `slave` e especifique um servidor de nomes que administre essa zona como `master` (que, por sua vez, pode ser uma escrava de outra master), como mostrado no Exemplo 40.5, “Entrada da zona para other-domain.de” (p 647).

Exemplo 40.5 *Entrada da zona para other-domain.de*

```
zone "other-domain.de" in {
type slave;
file "slave/other-domain.zone";
masters { 10.0.0.1; };
};
```

As opções de zona:

type master;
Ao especificar `master`, comunique ao BIND que a zona é gerenciada pelo servidor de nomes local. Esse procedimento pressupõe que um arquivo de zona tenha sido criado no formato correto.

type slave;
Esta zona é transferida de outro servidor de nomes. Ela deve ser usada juntamente com `masters`.

type hint;
A zona `.` do tipo `hint` é usada para definir os servidores de nomes raiz. Essa definição de zona pode ser deixada assim.

arquivo `my-domain.zone` ou arquivo "slave/other-domain.zone";
Esta entrada especifica o arquivo em que os dados da zona para o domínio estão localizados. Este arquivo não é necessário para uma escrava, pois os dados são buscados em outro servidor de nomes. Para diferenciar arquivos master de escravos, use o diretório `slave` para os arquivos escravos.

masters { *`endereço-ip-servidor`*; };
Esta entrada só é necessária para zonas escravas. Ela especifica o servidor de nomes do qual o arquivo da zona deve ser transferido.

allow-update {! *; };
Esta opção controla o acesso de gravação externo, permitindo que os clientes façam uma entrada no DNS, o que normalmente não é desejável por razões de segurança. Sem essa entrada, as atualizações da zona não são permitidas. A entrada acima obtém o mesmo porque `! *` proíbe efetivamente qualquer atividade afim.

40.5 Arquivos de zona

São necessários dois tipos de arquivos de zona. Um designa endereços IP a nomes de hosts e o outro faz o oposto: fornece um nome de host a um endereço IP.

DICA: Usando o ponto em arquivos de zona

O `.` tem um significado importante nos arquivos de zona. Se os nomes de host forem designados sem um `.` final, a zona será anexada. Nomes de host completos especificados sem um nome de domínio completo devem terminar com um `.` para evitar que o domínio seja adicionado a eles novamente. Pontos ausentes ou colocados erradamente são provavelmente a causa mais freqüente de erros de configuração do servidor de nomes.

O primeiro caso a considerar é o arquivo de zona `world.zone`, responsável pelo domínio `world.cosmos`, exibido no Exemplo 40.6, “Arquivo /var/lib/named/world.zone” (p 648).

Exemplo 40.6 *Arquivo /var/lib/named/world.zone*

```
$TTL 2D
world.cosmos. IN SOA      gateway  root.world.cosmos. (
            2003072441  ; serial
            1D          ; refresh
            2H          ; retry
            1W          ; expiry
            2D )        ; minimum

            IN NS       gateway
            IN MX       10 sun

gateway     IN A        192.168.0.1
            IN A        192.168.1.1
sun         IN A        192.168.0.2
moon        IN A        192.168.0.3
earth       IN A        192.168.1.2
mars        IN A        192.168.1.3
www         IN CNAME    moon
```

Linha 1:

`$TTL` define o tempo padrão de operação a ser aplicado em todas as entradas deste arquivo. Neste exemplo, as entradas são válidas por um período de dois dias (`2 D`).

Linha 2:
Onde o registro de controle SOA (start of authority) é iniciado:

- O nome do domínio a ser administrado é `world.cosmos` na primeira posição. Ele termina com um `.`, caso contrário a zona seria anexada outra vez. Como alternativa, é possível inserir uma `@` aqui, caso em que a zona seria extraída da entrada correspondente em `/etc/named.conf`.

- Depois, `IN SOA` será o nome do servidor de nomes master dessa zona. O nome é expandido de `gateway` para `gateway.world.cosmos`, pois ele não termina com um `.`.

- Depois, é exibido o endereço de e-mail da pessoa responsável por esse servidor de nomes. Como o sinal de `@` já tem um significado especial, o `.` é inserido aqui, no lugar dele. Para `root@world.cosmos`, a entrada deve ser lida como `root.world.cosmos.`. O `.` deve ser incluído no fim para evitar que a zona seja adicionada.

- O `(` inclui todas as linhas até `)`, no registro do SOA.

Linha 3:
O `serial number` é um número arbitrário que é aumentado sempre que o arquivo é mudado. Ele é necessário para informar os servidores de nomes secundários (servidores escravos) sobre as mudanças. Para isso, um número de 10 dígitos com a data e um número de execução, escrito como YYYYMMDDNN , é o formato mais usado.

Linha 4:
A `refresh rate` especifica o intervalo de tempo no qual os servidores de nomes secundários verificam o `serial number` da zona. Neste caso, um dia:

Linha 5:
`retry rate` especifica o intervalo de tempo no qual um servidor de nomes secundário tenta entrar em contato com o servidor primário novamente, no caso de erro. Aqui, duas horas.

Linha 6:
O `expiration time` especifica o intervalo de tempo no qual um servidor de nomes secundário descarta os dados em cache, caso não tenha conseguido restabelecer contato com o servidor primário. Aqui, uma semana.

Linha 7:

A última entrada do registro de SOA especifica o `negative caching TTL` — o tempo em que resultados de consultas não resolvidas do DNS de outros servidores podem ser armazenados em cache.

Linha 9:

O `IN NS` especifica o servidor de nomes responsável por este domínio. `gateway` é estendido para `gateway.world.cosmos`, pois não termina com um `.`. Pode haver várias linhas como esta: uma para o servidor de nomes primário e outra para o secundário. Se `notify` não for enviado para `no` em `/etc/named.conf`, todos os servidores de nomes listados aqui serão informados sobre as mudanças feitas nos dados da zona.

Linha 10:

O registro MX especifica o servidor de correio eletrônico que aceita, processa e encaminha e-mails para o domínio `world.cosmos`. Neste exemplo, o host é `sun.world.cosmos`. O número na frente do nome do host é o valor de preferência. Se houver várias entradas de MX, o servidor de correio eletrônico com menor valor será pego primeiro e se houver falha na entrega de mensagens, será feita uma nova tentativa com o próximo valor mais alto.

Linhas 12 a 17:

Estes são os registros reais em que um ou mais endereços IP são atribuídos a nomes de host. Os nomes são listados aqui sem um `.`, pois eles não incluem seus domínios, então `world.cosmos` é adicionado a todos. Dois endereços IP são designados ao host `gateway`, pois ele tem duas placas de rede. Em todos os locais em que o endereço de host for tradicional (IPv4), o registro será marcado com `A`. Se o endereço for um endereço IPv6, a entrada será marcada com `A6`. O token anterior para os endereços IPv6 era `AAAA`, agora obsoleto.

Linha 18:

O álias `www` pode ser usado como endereço `mond` (`CNAME` significa *nome canônico*).

O pseudodomínio `in-addr.arpa` é usado para a pesquisa reversa de endereços IP em nomes de hosts. Ele é anexado à parte de rede do endereço, em notação reversa. Então, `192.168.1` é resolvido como `1.168.192.in-addr.arpa`. Consulte Exemplo 40.7, “Pesquisa reversa” (p 651).

Exemplo 40.7 *Pesquisa reversa*

```
 $TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.world.cosmos. root.world.cosmos. (
                        2003072441      ; serial
                        1D              ; refresh
                        2H              ; retry
                        1W              ; expiry
                        2D )            ; minimum

                        IN NS           gateway.world.cosmos.

1                       IN PTR          gateway.world.cosmos.
2                       IN PTR          earth.world.cosmos.
3                       IN PTR          mars.world.cosmos.
```

Linha 1:
STLL define o TTL padrão aplicado a todas as entradas aqui.

Linha 2:
O arquivo de configuração deve ativar a pesquisa reversa para a rede `192.168.1.0`. Supondo que a zona seja chamada de `1.168.192.in-addr.arpa`, ela não deve ser adicionada a nomes de hosts. Portanto, todos os nomes de host são digitados na forma completa, com seu domínio e um `.` no fim. As entradas restantes correspondem às descritas no exemplo de `world.cosmos` anterior.

Linhas 3 a 7:
Consulte o exemplo anterior para `world.cosmos`.

Linha 9:
Novamente, esta linha especifica o servidor de nomes responsável pela zona. No entanto, dessa vez o nome é digitado na forma completa, com o domínio e um `.` no fim.

Linhas 11 a 13:
Estas são as dicas dos registros do indicador nos endereços IP dos respectivos hosts. Somente a última parte do endereço IP é digitada no começo da linha, sem o `.` no fim. Anexar a zona a ele (sem `.in-addr.arpa`) resulta na ordem reversa de todo o endereço IP.

Normalmente, as transferências de zona entre versões diferentes do BIND devem ser possíveis sem problemas.

40.6 Atualização dinâmica dos dados da zona

O termo *atualização dinâmica* se refere a operações pelas quais as entradas dos arquivos de zona de um servidor master são adicionadas, mudadas ou apagadas. Esse mecanismo é descrito no RFC 2136. A atualização dinâmica é configurada individualmente para cada entrada de zona, se você adicionar uma regra `allow-update` ou `update-policy` opcional. As zonas a serem atualizadas dinamicamente não devem ser editadas manualmente.

Transmita as entradas a serem atualizadas para o servidor com o comando `nsupdate`. Para obter a sintaxe exata deste comando, verifique a página de manual correspondente a nsupdate (`man 8 nsupdate`). Por razões de segurança, qualquer atualização desse tipo deve ser executada com chaves TSIC, conforme descrito na Seção 40.7, “Transações de segurança” (p 652).

40.7 Transações de segurança

Transações seguras podem ser feitas com a ajuda de TSIGs (Transaction Signatures, Assinaturas de Transação), baseadas em chaves secretas compartilhadas (também chamadas de chaves TSIGs). Esta seção descreve como gerar e usar tais chaves.

Transações seguras são necessárias para a comunicação entre servidores diferentes e para a atualização dinâmica dos dados de zona. Tornar o controle de acesso dependente de chaves é muito mais seguro do que meramente confiar em endereços IP.

Gere uma chave TSIG com o seguinte comando (para obter detalhes, consulte `man dnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Serão criados dois arquivos com nomes similares a:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

A chave (uma string como `ejIkuCyyGJwwuN3xAteKgg==`) é encontrada nos dois arquivos. Para usá-la em transações, o segundo arquivo (`Khost1-host2.+157+34265.key`) deve ser transferido para o host remoto, de preferência de forma segura

(usando scp, por exemplo). No servidor remoto, a chave deve ser incluída no arquivo `/etc/named.conf` para permitir uma comunicação segura entre `host1` e `host2`:

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

ATENÇÃO: Permissões de arquivo de `/etc/named.conf`

Verifique se as permissões do arquivo `/etc/named.conf` foram restringidas adequadamente. O padrão para esse arquivo é `0640`, com o proprietário sendo `root` e o grupo, `named`. Como alternativa, mova as chaves para um outro arquivo com permissões especialmente limitadas, que então será incluído de `/etc/named.conf`.

Para permitir que o servidor `host1` use a chave para `host2` (que tem o endereço `192.168.2.3` neste exemplo), o arquivo `/etc/named.conf` do servidor deve incluir a seguinte regra:

```
server 192.168.2.3 {
 keys { host1-host2. ;};
};
```

Entradas análogas devem ser incluídas nos arquivos de configuração de `host2`.

Adicione chaves TSIG a quaisquer ACLs (listas de controle de acesso, não confundir com as ACLs do sistema de arquivos) definidas por endereços IP e intervalos de endereço para possibilitar a segurança da transação. A entrada correspondente deve ter esta aparência:

```
allow-update { key host1-host2. ;};
```

Este tópico é discutido com mais detalhes no *BIND Administrator Reference Manual* (Manual de Referência do Administrador BIND), em `update-policy`.

40.8 Segurança do DNS

A DNSSEC, ou segurança do DNS, é descrita no RFC 2535. As ferramentas disponíveis para a DNSSEC serão discutidas no Manual do BIND.

Uma zona considerada segura deve ter uma ou mais chaves associadas a ela. Elas são geradas com o comando `dnssec-keygen`, assim como as chaves do host. O algoritmo de criptografia de DSA é usado atualmente para gerar essas chaves. As chaves públicas geradas devem ser incluídas no arquivo de zona correspondente, com uma regra `$INCLUDE`.

Com o comando `dnssec-makekeyset`, todas as chaves geradas são empacotadas em um conjunto, que deve ser transferido para a zona-pai de forma segura. Na zona-pai, o conjunto é assinado com `dnssec-signkey`. Os arquivos gerados por esse comando são usados para assinar as zonas com o comando `dnssec-signzone`, que por sua vez gera os arquivos a serem incluídos em cada zona de `/etc/named.conf`.

40.9 Para obter mais informações

Para obter mais informações, consulte o *BIND Administrator Reference Manual* (Manual de Referência do Administrador do BIND), que está instalado em `/usr/share/doc/packages/bind/`. Considere ainda consultar os RFCs citados pelo manual e as páginas de manual incluídas no BIND. O arquivo `/usr/share/doc/packages/bind/README.SuSE` contém informações atualizadas sobre o BIND no SUSE Linux.

41 Usando o NIS

Assim que vários sistemas UNIX em uma rede desejam acessar recursos comuns, torna-se muito importante que todas as identidades de usuário e grupo sejam a mesma para todas as máquinas nessa rede. A rede deve ser transparente para os usuários: qualquer que seja a máquina que estiverem usando, sempre se encontrarão exatamente no mesmo ambiente. Isso é possível através dos serviços do NIS e do NFS. O NFS distribui sistemas de arquivos em uma rede e é discutido no Capítulo 42, *Compartilhando sistemas de arquivos com o NFS* (p 663).

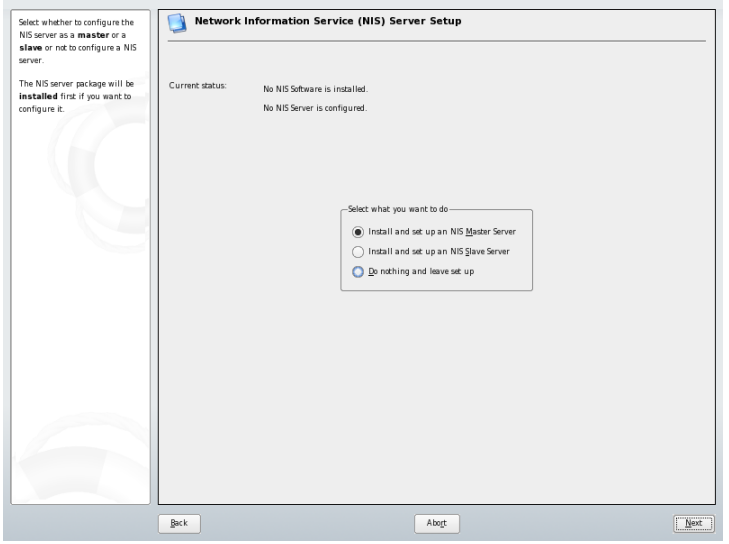
O NIS (Network Information Service - Serviço de Informações de Rede) pode ser descrito como um serviço parecido com um banco de dados que fornece acesso ao conteúdo de `/etc/passwd`, `/etc/shadow` e `/etc/group` através de redes. O NIS também pode ser usado para outros fins (disponibilizar o conteúdo de arquivos como `/etc/hosts` ou `/etc/services`, por exemplo), mas isso está além do escopo dessa introdução. As pessoas, normalmente, referem-se ao NIS como *YP* (Yellow Pages - Páginas Amarelas), pois ele funciona como se fosse as “páginas amarelas” da rede.

41.1 Configurando servidores NIS usando o YaST

Para configurar, selecione *Servidor NIS* no módulo *Serviços de Rede* do YaST. Se ainda não houver servidor NIS em sua rede, ative *Instalar e configurar servidor de NIS Mestre* na tela a seguir. O YaST instalará imediatamente os pacotes solicitados.

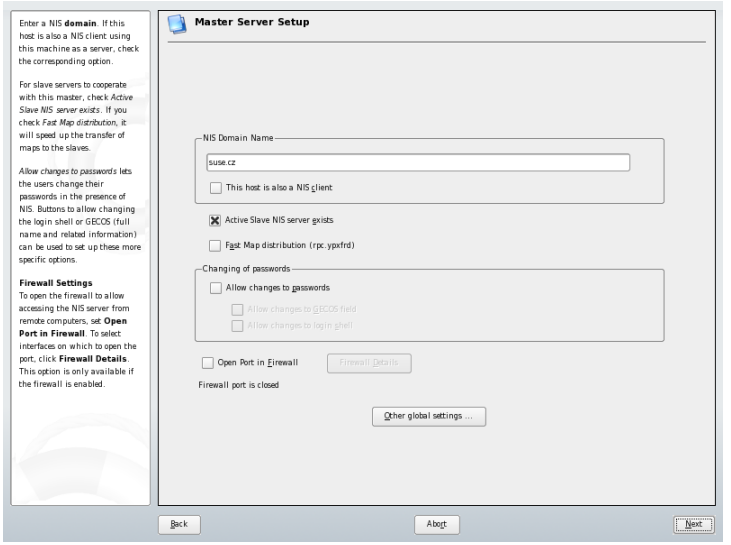
Se você já tiver instalado o software NIS, clique em *Criar um servidor de NIS Mestre*. Se você já tiver um servidor NIS (um *master*), poderá adicionar um servidor NIS escravo (por exemplo, se desejar configurar uma nova sub-rede). Primeiro, é descrita a configuração do servidor master. Se clicar em *Não fazer nada e abandonar a configuração*, você retornará ao Centro de Controle do YaST sem ter gravado as mudanças.

Figura 41.1 *Configuração do servidor NIS*


Select whether to configure the NIS server as a master or a slave or not to configure a NIS server.
The NIS server package will be installed first if you want to configure it.
Network Information Service (NIS) Server Setup
Current status:
No NIS Software is installed.
No NIS Server is configured.
Select what you want to do
Install and set up an NIS Master Server
Install and set up an NIS Slave Server
Do nothing and leave set up
Back
Abort
Next

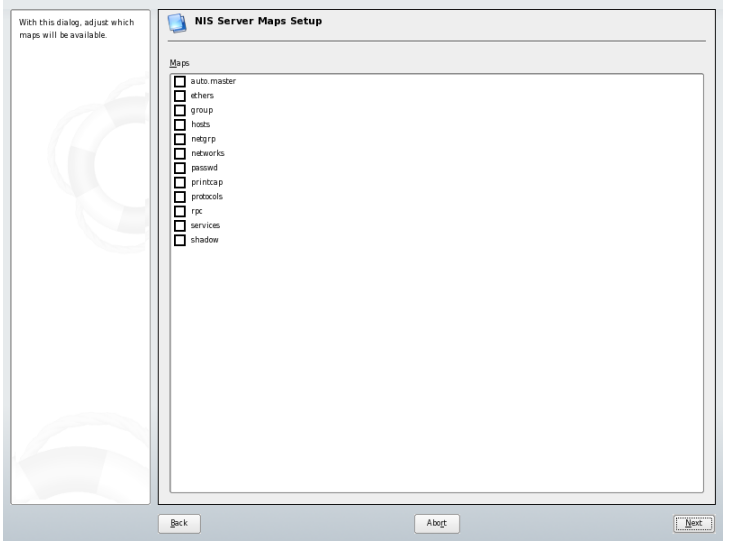
Uma vez instalados todos os pacotes, digite o nome de domínio do NIS na parte superior da caixa de diálogo de configuração, mostrada na Figura 41.1, “Configuração do servidor NIS” (p 656). Na caixa de seleção, defina se o host também deve ser um cliente NIS, possibilitando que usuários efetuem login e acessem dados no servidor NIS. Marque as caixas que deseja aplicar, incluindo a opção *Mudança de senhas*. Opções adicionais podem ser definidas clicando em *Outras configurações globais*. Aqui, você acessa uma tela na qual pode mudar o diretório de origem, mesclar senhas e definir um mínimo de IDs de grupo e usuário. Clique em *OK* para retornar à caixa de diálogo principal. Clique em *Próximo* para continuar a configuração.

Figura 41.2 *Configuração de servidor master*


Enter a NIS **domain**. If this host is also a NIS client using this machine as a server, check the corresponding option.
For slave servers to cooperate with this master, check *Active Slave NIS server exists*. If you check *Fast Map distribution*, it will speed up the transfer of maps to the slaves.
Allow changes to passwords lets the users change their passwords in the presence of NIS. Buttons to allow changing the login shell or GECOS (full name and related information) can be used to set up these more specific options.
Firewall Settings
To open the firewall to allow accessing the NIS server from remote computers, set **Open Port in Firewall**. To select interfaces on which to open the port, click **Firewall Details**. This option is only available if the firewall is enabled.
Master Server Setup
NIS Domain Name
suse.cz
This host is also a NIS client
Active Slave NIS server exists
Fast Map distribution (rpc.ypxfrd)
Changing of passwords
Allow changes to passwords
Allow changes to GECOS field
Allow changes to login shell
Open Port in Firewall
Firewall Details
Firewall port is closed
Other global settings ...
Back
Abort
Next

Na tela a seguir, especifique quais mapas devem ficar disponíveis. Ao clicar em *Próximo*, você entra na tela seguinte, na qual determina quais hosts podem consultar o servidor NIS. Você pode adicionar, apagar e editar hosts. Clique em *Concluir* para gravar as mudanças e sair da caixa de diálogo de configuração.

Figura 41.3 *Configuração de mapas do servidor NIS*



Para configurar NIS adicionais (*servidores escravos*) na sua rede, ative *Instalar e configurar servidor de NIS Escravo* agora. Se o software NIS já tiver sido instalado, clique em *Criar um servidor de NIS Escravo* e em *Próximo* para continuar. Na tela seguinte, digite o nome de domínio NIS e marque as caixas que se aplicam a ele.

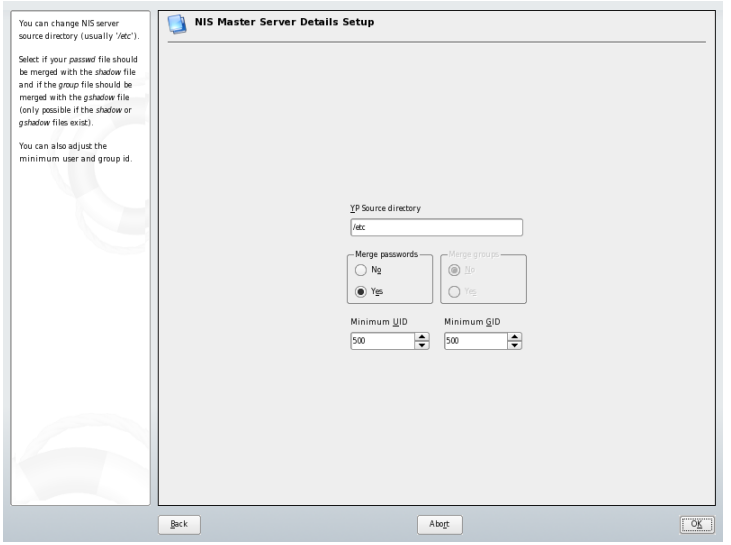
Para permitir que os usuários da rede (tanto usuários locais quanto os gerenciados pelo servidor NIS) mudem suas senhas no servidor NIS (com o comando `yppasswd`), ative a opção correspondente. Isso disponibiliza as opções *Permitir mudanças no campo GECOS* e *Permitir mudanças no shell de login*. "GECOS" significa que os usuários também podem mudar suas configurações de endereço e nomes com o comando `ypchfn`. "SHELL" permite que os usuários mudem seu shell padrão com o comando `ypchsh`, por exemplo, para alternar de bash para sh.

Opções adicionais podem ser definidas clicando em *Outras configurações globais*. Aqui você acessa uma tela, mostrada na Figura 41.4, "Mudando o diretório e sincronizando arquivos para um servidor NIS" (p 659), em que você pode mudar o diretório de origem do servidor NIS (`/etc` por padrão). Além disso, senhas e grupos podem ser mesclados aqui. A configuração deve ser *Sim*, para que os arquivos (`/etc/passwd`, `/etc/shadow` e `/etc/group`) possam ser sincronizados. Determine também o menor ID de grupo e usuário. Clique em *OK* para confirmar suas configurações e retorne à tela anterior.

Após concluir suas configurações, avance para a tela seguinte, clicando em *Próximo*. Na caixa de diálogo seguinte, marque quais mapas estarão disponíveis e, depois, clique em *Próximo* para continuar. Na última tela, digite quais hosts podem consultar o servidor NIS. Você pode adicionar, editar ou apagar hosts, clicando nos botões adequados. Clique em *Concluir*, para gravar as mudanças e sair da configuração.

Depois, clique em *Próximo*.

Figura 41.4 *Mudando o diretório e sincronizando arquivos para um servidor NIS*


You can change NIS server source directory (usually '/etc').
Select if your passwd file should be merged with the shadow file and if the group file should be merged with the gshadow file (only possible if the shadow or gshadow files exist).
You can also adjust the minimum user and group id.
NIS Master Server Details Setup
YP Source directory
/etc
Merge passwords
No
Yes
Merge groups
No
Yes
Minimum UID
500
Minimum GID
500
Back
Abort
OK

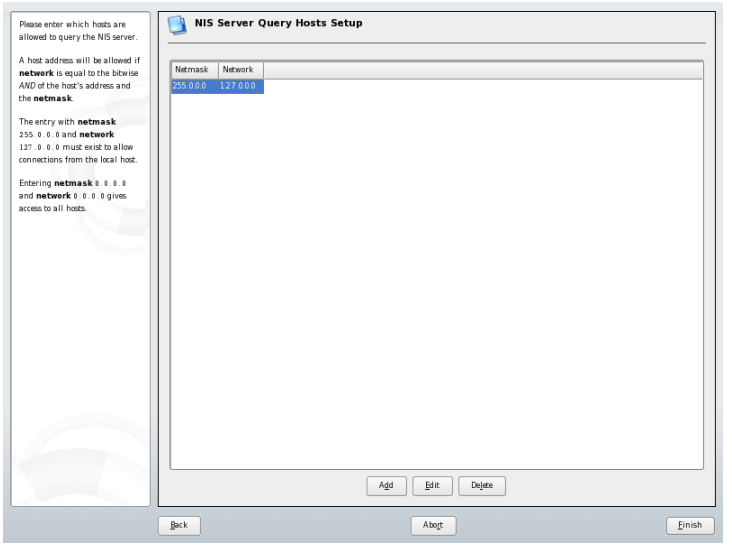
Se você habilitou anteriormente a opção *Existe um servidor de NIS escravo ativo*, digite os nomes de host usados como escravos e clique em *Próximo*. Se você não usa servidores escravos, a configuração escrava é ignorada e você continuará diretamente na caixa de diálogo para a configuração do banco de dados. Aqui, especifique os *mapas*, os bancos de dados parciais a serem transferidos do servidor NIS para o cliente. As configurações padrão geralmente são adequadas.

Próximo continua até a última caixa de diálogo, mostrada na Figura 41.5, “Configurando permissões de solicitação para um servidor NIS” (p 660). Especifique de quais redes as solicitações podem ser enviadas para o servidor NIS. Normalmente, esta é sua rede interna. Nesse caso, deve haver as duas entradas a seguir:

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

A primeira entrada habilita conexões do seu próprio host, que é o servidor NIS. A segunda permite que todos os hosts com acesso à mesma rede enviem solicitações ao servidor.

Figura 41.5 *Configurando permissões de solicitação para um servidor NIS*


Please enter which hosts are allowed to query the NIS server.
A host address will be allowed if network is equal to the bitwise AND of the host's address and the netmask.
The entry with netmask 255.0.0.0 and network 127.0.0.0 must exist to allow connections from the local host.
Entering netmask 0.0.0.0 and network 0.0.0.0 gives access to all hosts.
NIS Server Query Hosts Setup
Netmask
Network
255.0.0.0
127.0.0.0
Add
Edit
Delete
Back
Abort
Finish

IMPORTANTE: Configuração automática de firewall

Se um firewall estiver ativo no seu sistema (SuSEfirewall2), o YaST adaptará sua configuração para o servidor NIS habilitando o serviço `portmap` quando *Abrir Portas no Firewall* for selecionado.

41.2 Configurando clientes NIS

Use este módulo para configurar um cliente NIS. Depois de escolher usar o NIS e, dependendo das circunstâncias, o automontador, essa caixa de diálogo se abrirá. Selecione se o host possui um endereço IP estático ou se recebe um emitido pelo DHCP. O DHCP também fornece o domínio NIS e o servidor NIS. Para obter mais informações sobre o DHCP, consulte o Capítulo 43, *DHCP* (p 669). Se um endereço IP estático for usado, especifique o domínio NIS e o servidor NIS manualmente. Consulte a Figura 41.6, “Definindo o domínio e o endereço de um servidor NIS” (p 661). *Procurar* faz o YaST

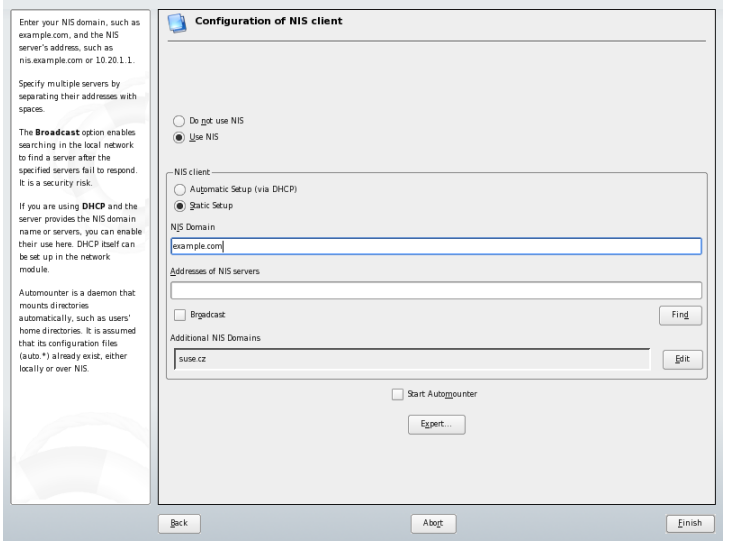
procurar um servidor NIS ativo na rede. *Broadcast* habilita a procura na rede local por um servidor quando não há resposta dos servidores especificados.

Você também pode especificar vários servidores, digitando seus endereços em *Endereços IP dos servidores NIS* e separando-os com espaços.

Nas configurações avançadas, desabilite a opção *Responder aos Hosts Remotos* para que outros hosts não possam consultar o servidor usado pelo seu cliente. Ao marcar a opção *Servidor Estragado*, o cliente poderá receber respostas de um servidor que se comunica por uma porta sem privilégio. Para obter mais informações, consulte `man ypbind`.

Ao terminar suas configurações, clique em *Concluir* para mudá-las e retornar ao Centro de Controle do YaST.

Figura 41.6 *Definindo o domínio e o endereço de um servidor NIS*


Enter your NIS domain, such as example.com, and the NIS server's address, such as nis.example.com or 10.20.1.1.
Specify multiple servers by separating their addresses with spaces.
The Broadcast option enables searching in the local network to find a server after the specified servers fail to respond. It is a security risk.
If you are using DHCP and the server provides the NIS domain name or servers, you can enable their use here. DHCP itself can be set up in the network module.
Automounter is a daemon that mounts directories automatically, such as users' home directories. It is assumed that its configuration files (auto.*) already exist, either locally or over NIS.
Configuration of NIS client
Do not use NIS
Use NIS
NIS client
Automatic Setup (via DHCP)
Static Setup
NIS Domain
example.com
Addresses of NIS servers
Broadcast
Find
Additional NIS Domains
suse.cz
Edit
Start Automounter
Expert...
Back
Abort
Finish

Compartilhando sistemas de arquivos com o NFS

42

Como mencionado no Capítulo 41, *Usando o NIS* (p 655), o NFS funciona com o NIS para tornar uma rede transparente para o usuário. Com o NFS, é possível distribuir sistemas de arquivos pela rede. Não importa em qual terminal os usuários estão conectados. Eles sempre se encontram no mesmo ambiente.

Da mesma forma que o NIS, o NFS é um serviço assimétrico. Há servidores NFS e clientes NFS. Uma máquina pode ser ambos — pode fornecer sistemas de arquivos pela rede (exportar) e montar sistemas de arquivos a partir de outros hosts (importar). Geralmente, há servidores com um disco rígido cuja capacidade é bem grande e cujos sistemas de arquivos são montados por outros clientes.

IMPORTANTE: Necessidade do DNS

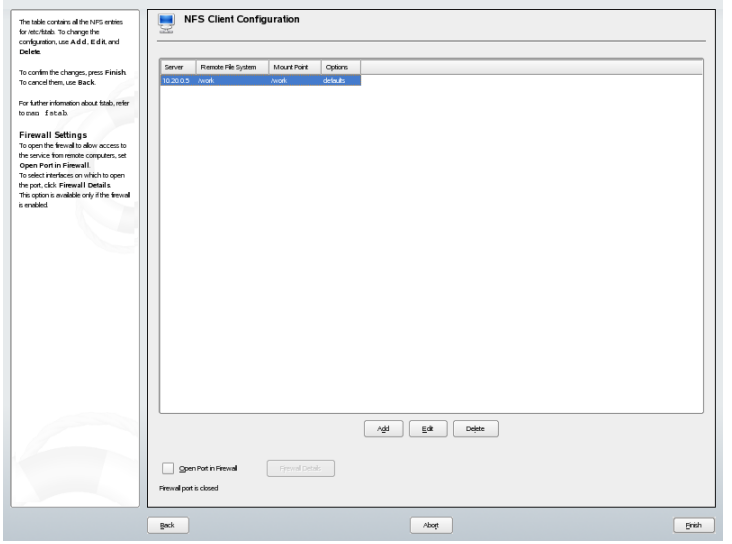
A princípio, todas as exportações podem ser feitas usando somente endereços IP. Para evitar tempos de espera, você deve ter um sistema DNS em funcionamento. Isso é necessário pelo menos para fins de registro, pois o daemon montado inverte pesquisas.

42.1 Importando sistemas de arquivos com o YaST

Usuários autorizados para fazer isso podem montar diretórios NFS a partir de um servidor NFS em suas próprias árvores de arquivos. Isso pode ser feito mais facilmente usando o módulo YaST *Cliente NFS*. Basta digitar o nome de host do servidor NFS, o

diretório a ser importado e o ponto de montagem no qual esse diretório deve ser montado localmente. Tudo isso é feito depois de você clica em *Adicionar* na primeira caixa de diálogo. Clique em *Abrir Porta no Firewall* para abrir o firewall e permitir que computadores remotos acessem o serviço. O status do firewall é mostrado próximo à caixa de seleção. Ao clicar em *OK*, você grava suas mudanças. Consulte a Figura 42.1, “Configuração do cliente NFS com o YaST” (p 664).

Figura 42.1 *Configuração do cliente NFS com o YaST*



42.2 Importando sistemas de arquivos manualmente

Os sistemas de arquivos podem ser facilmente importados manualmente de um servidor NFS. O único pré-requisito é executar um mapeador de porta RPC, que pode ser iniciado digitando o comando `rcportmap start` como `root`. Depois que esse pré-requisito é executado, os sistemas de arquivos remotos exportados nas respectivas máquinas podem ser montados no sistema de arquivos da mesma forma que discos rígidos locais, usando o comando `mount` com a seguinte sintaxe:

```
mount host:remote-path local-path
```

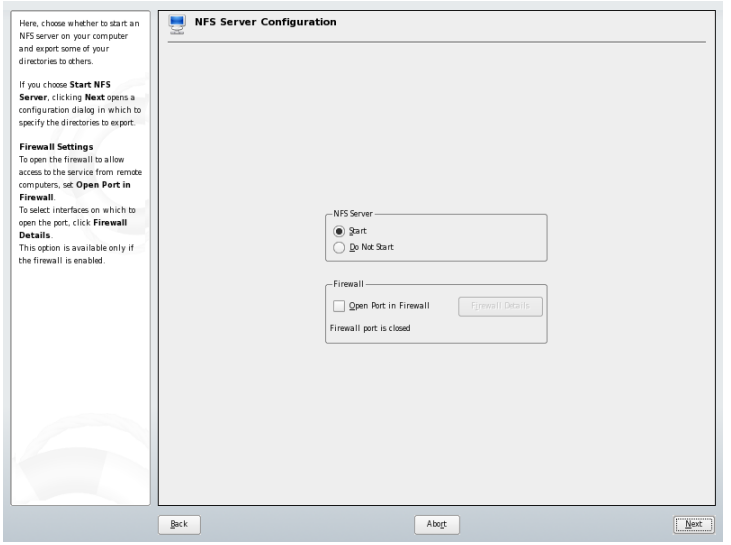
Se os diretórios de usuário da máquina sun, por exemplo, precisarem ser importados, use o seguinte comando:

```
mount sun:/home /home
```

42.3 Exportando sistemas de arquivos com o YaST

Com o YaST, transforme um host de sua rede em um servidor NFS — um servidor que exporta diretórios e arquivos para todos os hosts aos quais ele concede acesso. Isso poderia ser feito para fornecer aplicativos a todos os membros de um grupo, sem instalá-los localmente em cada um dos hosts. Para instalar um servidor como esse, inicie o YaST e selecione *Serviços de Rede* → *Servidor NFS*. Uma caixa de diálogo como a da Figura 42.2, “Ferramenta de configuração do servidor NFS” (p 665) é exibida.

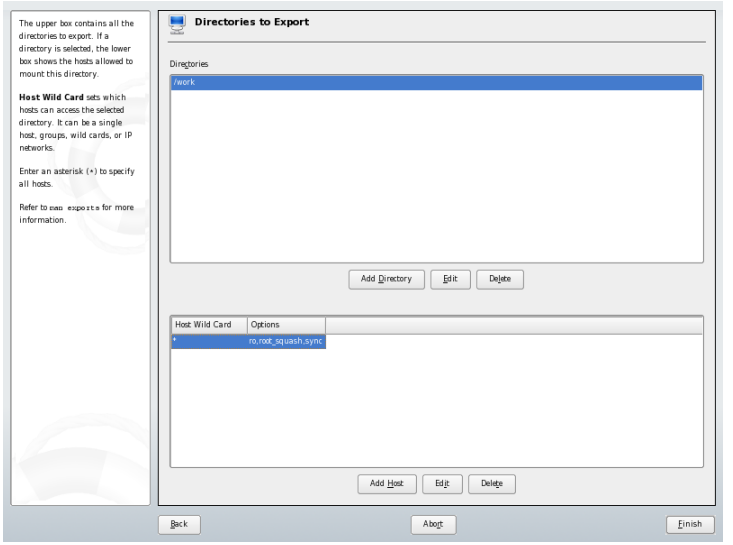
Figura 42.2 *Ferramenta de configuração do servidor NFS*


Here, choose whether to start an NFS server on your computer and export some of your directories to others.
If you choose Start NFS Server, clicking Next opens a configuration dialog in which to specify the directories to export.
Firewall Settings
To open the firewall to allow access to the service from remote computers, set Open Port in Firewall.
To select interfaces on which to open the port, click Firewall Details.
This option is available only if the firewall is enabled.
NFS Server Configuration
NFS Server
Start
Do Not Start
Firewall
Open Port in Firewall
Firewall Details...
Firewall port is closed
Back
Abort
Next

Em seguida, ative *Iniciar Servidor NFS* e clique em *Próximo*. No campo de texto superior, digite os diretórios a serem exportados. Abaixo, digite os hosts que devem ter acesso a eles. Essa caixa de diálogo é mostrada na Figura 42.3, “Configurando um servidor NFS com o YaST” (p 666). Há quatro opções que podem ser configuradas para

cada host: `host único`, `grupos de rede`, `curingas` e `redes IP`. Uma explicação mais detalhada dessas opções é fornecida por `man exports`. *Sair* conclui a configuração.

Figura 42.3 *Configurando um servidor NFS com o YaST*


The upper box contains all the directories to export. If a directory is selected, the lower box shows the hosts allowed to mount this directory.
Host Wild Card sets which hosts can access the selected directory. It can be a single host, groups, wild cards, or IP networks.
Enter an asterisk (*) to specify all hosts.
Refer to man exports for more information.
Directories to Export
Directories
/work
Add Directory
Edit
Delete
Host Wild Card
Options
*
ro,root_squash,sync
Add Host
Edit
Delete
Back
Abort
Finish

IMPORTANTE: Configuração automática de firewall

Se um firewall estiver ativo no seu sistema (SuSEfirewall2), o YaST adaptará sua configuração para o servidor NFS habilitando o serviço `nfs` quando *Abrir Portas no Firewall* for selecionado.

42.4 Exportando sistemas de arquivos manualmente

Se não você deseja usar o YaST, verifique se os sistemas a seguir podem ser executados no servidor NFS:

- portmapper RPC (portmap)

- daemon de montagem do RPC (rpc.mountd)
- daemon NFS do RPC (rpc.nfsd)

Para que esses serviços sejam iniciados pelos scripts `/etc/init.d/portmap` e `/etc/init.d/nfsserver` quando o sistema for inicializado, digite os comandos `insserv /etc/init.d/nfsserver` e `insserv /etc/init.d/portmap`. Defina também quais sistemas de arquivos devem ser exportados para que hosts do arquivo de configuração `/etc/exports`.

Para que cada diretório possa exportar, uma linha é necessária para configurar as máquinas que podem acessar esse diretório com determinadas permissões. Todos os subdiretórios desse diretório também são automaticamente exportados. As máquinas autorizadas são normalmente especificadas com seus nomes completos (incluindo o nome de domínio), mas é possível usar curingas como `*` ou `?` (que se expandem da mesma forma que o shell Bash). Se nenhuma máquina for especificada aqui, qualquer máquina poderá importar esse sistema de arquivos com as permissões fornecidas.

Configure as permissões entre colchetes após o nome da máquina para o sistema de arquivos a ser exportado. As opções mais importantes são mostradas na Tabela 42.1, “Permissões para sistema de arquivos exportados” (p 667).

Tabela 42.1 *Permissões para sistema de arquivos exportados*

opção	significado
`ro`	O sistema de arquivos é exportado com permissão Apenas Leitura (padrão).
`rw`	O sistema de arquivos é exportado com permissão leitura-gravação.
`root_squash`	Isso garante que o usuário `root` de uma máquina importada não possua permissões `root` nesse sistema de arquivos. Isso pode ser feito designando o ID de usuário `65534` a usuários com o ID `0` (`root`). Esse ID de usuário deve ser configurado como `nobody` (que é o padrão).
`no_root_squash`	Não designa o ID de usuário `0` ao ID de usuário `65534`, mantendo as permissões de `root` válidas.

opção	significado
`link_relative`	Converte links absolutos (os que iniciam com `/`) em uma seqüência de `../`. Isso só terá utilidade se todo o sistema de arquivos de uma máquina estiver montado (padrão).
`link_absolute`	Os links simbólicos permanecem intactos.
`map_identity`	Os IDs de usuário são exatamente os mesmos no cliente e no servidor (padrão).
`map_daemon`	Cliente e servidor não possuem IDs de usuário correspondentes. Isso faz com que o nfsd crie uma tabela de conversão para IDs de usuário. O daemon ugidd é necessário para que isso funcione.

Seu arquivo `exportações` talvez fique parecido com o Exemplo 42.1, "/etc/exports" (p 668). `/etc/exports` é lido por mountd e nfsd. Se você fizer mudanças nesse arquivo, reinicie mountd e nfsd para que elas sejam efetivadas. Isso pode ser feito facilmente com o `rcnfsserver restart`.

Exemplo 42.1 */etc/exports*

```
#
# /etc/exports
#
/home             sun(rw)    venus(rw)
/usr/X11          sun(ro)    venus(ro)
/usr/lib/texmf    sun(ro)    venus(rw)
/                 earth(ro,root_squash)
/home/ftp         (ro)
# End of exports
```

43

DHCP

A finalidade do *DHCP* é designar configurações de redes de forma central, a partir de um servidor, em vez de defini-las localmente em cada estação de trabalho. Um host configurado para usar o DHCP não tem controle sobre seu próprio endereço estático. Ele é habilitado para configurar a si mesmo de forma completa e automática, de acordo com as direções do servidor.

Uma forma de usar o DHCP é identificar cada cliente através do endereço de hardware de sua respectiva placa de rede (na maioria dos casos, fixa) e, então, fornecer a esse cliente configurações idênticas toda vez que ele se conectar ao servidor. O DHCP também pode ser configurado para que o servidor designe endereços a cada cliente interessado de forma dinâmica, a partir de um pool de endereços configurado para essa finalidade. No último caso, o servidor DHCP tenta designar o mesmo endereço ao cliente toda vez que ele recebe uma solicitação deste, mesmo durante períodos mais longos. Obviamente, isso só funciona enquanto a rede não tiver mais clientes do que endereços.

Com essas possibilidades, o DHCP pode facilitar a vida dos administradores de sistema de duas maneiras. Quaisquer mudanças, mesmo as maiores, relacionadas a endereços e à configuração de rede, geralmente podem ser implementadas de forma centralizada, editando o arquivo de configuração do servidor. Isso é mais conveniente do que reconfigurar inúmeras estações de trabalho. Também é muito mais fácil integrar máquinas, especialmente as mais novas, na rede, pois podem receber um endereço IP do pool. A recuperação de configurações de rede apropriadas de um servidor DHCP pode ser muito útil no caso de laptops regularmente usados em redes diferentes.

Um servidor DHCP não só fornece o endereço IP e a máscara de rede, como também os endereços do servidor de nomes, o nome de host, o nome de domínio e o gateway a

ser usado pelo cliente. Além disso, o DHCP permite que vários outros parâmetros sejam configurados de forma centralizada, por exemplo, um servidor de horários do qual clientes possam fazer poll do horário atual ou até mesmo um servidor de impressão.

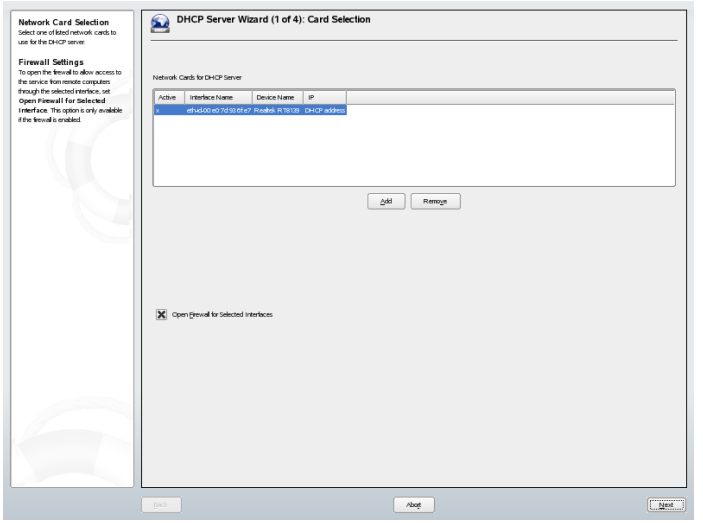
43.1 Configurando um servidor DHCP com o YaST

Quando o módulo é iniciado pela primeira vez, um assistente é iniciado, solicitando que você tome algumas decisões básicas referentes à administração do servidor. A conclusão dessa configuração inicial produz uma configuração de servidor muito básica, que deve funcionar com aspectos essenciais. O modo de especialista pode ser usado para lidar com tarefas de configuração mais avançadas.

Seleção de placa

Na primeira etapa, o YaST procura interfaces de rede disponíveis no sistema e, depois, mostra-as em uma lista. Na lista, selecione a interface em que o servidor DHCP deve escutar e clique em *Adicionar*e, em seguida, selecione *Abrir Firewall para Interfaces Selecionadas* a fim de abrir o firewall para essa interface. Consulte a Figura 43.1, “Servidor DHCP: seleção de placa” (p 670).

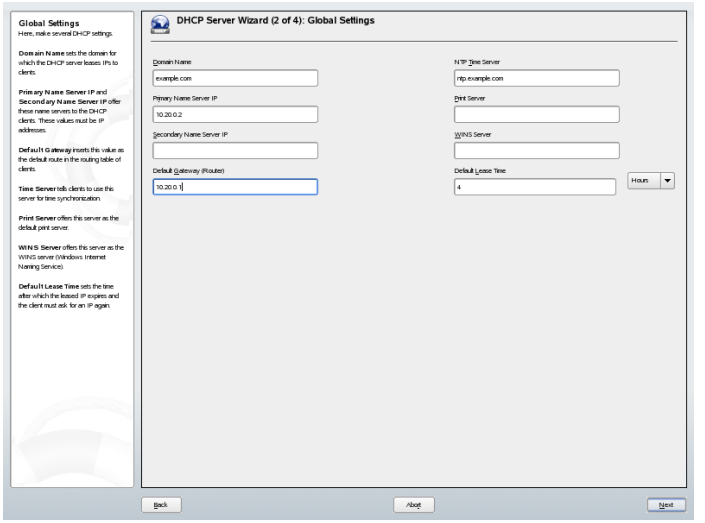
Figura 43.1 *Servidor DHCP: seleção de placa*


Network Card Selection
Select one of listed network cards to use for the DHCP server.
Firewall Settings
To open the firewall to allow access to the service from remote computers through the selected interface, set Open Firewall for Selected Interface. This option is only available if the firewall is enabled.
DHCP Server Wizard (1 of 4): Card Selection
Network Cards for DHCP Server
Active
Interface Name
Device Name
IP
Add
Remove
Open Firewall for Selected Interfaces
Back
Abort
Next

Configurações globais

Nos campos de entrada, forneça os detalhes da rede para todos os clientes que o servidor DHCP deve gerenciar. Esses detalhes são o nome de domínio, o endereço de um servidor de horário, os endereços do servidor de nomes primário e secundário, os endereços de um servidor WINS e de impressão (para uma rede mista com os clientes Windows e Linux), o endereço de gateway e o tempo de aluguel. Consulte a Figura 43.2, “Servidor DHCP: configurações globais” (p 671).

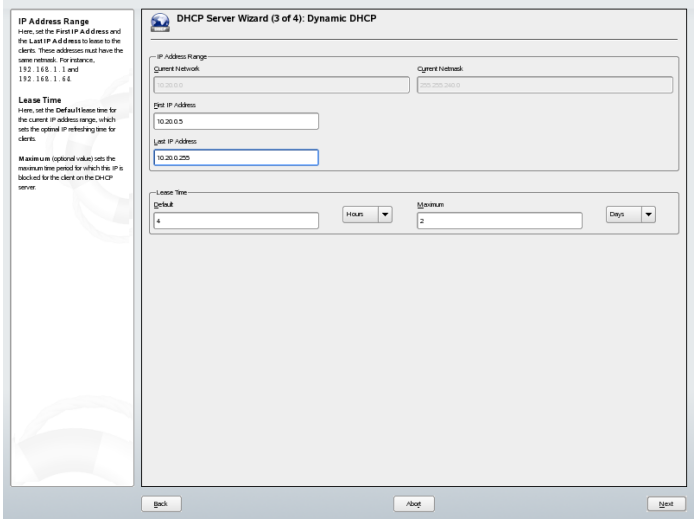
Figura 43.2 *Servidor DHCP: configurações globais*


Global Settings
Here, make several DHCP settings.
Domain Name sets the domain for which the DHCP server leases IPs to clients.
Primary Name Server IP and Secondary Name Server IP offer these name servers to the DHCP clients. These values must be IP addresses.
Default Gateway inserts this value as the default route in the routing table of clients.
Time Server tells clients to use this server for time synchronization.
Print Server offers this server as the default print server.
WINS Server offers this server as the WINS server (Windows Internet Naming Service).
Default Lease Time sets the time after which the leased IP expires and the client must ask for an IP again.
DHCP Server Wizard (2 of 4): Global Settings
Domain Name
example.com
Primary Name Server IP
10.20.0.2
Secondary Name Server IP
Default Gateway (Router)
10.20.0.1
NTP Time Server
ntp.example.com
Print Server
WINS Server
Default Lease Time
4
Hours
Back
Abort
Next

DHCP dinâmico

Nessa etapa, configure o nível de dinamismo dos endereços IP designados aos clientes. Para fazer isso, especifique uma faixa IP a partir da qual o servidor pode designar endereços a clientes DHCP. Todos esses endereços precisam ser cobertos pela mesma máscara de rede. Especifique também o tempo de aluguel durante o qual um cliente pode manter seu endereço IP sem precisar solicitar uma extensão do aluguel. Outra opção é especificar o tempo de aluguel máximo, que é o período durante o qual o servidor reserva um endereço IP para um cliente específico. Consulte a Figura 43.3, “Servidor DHCP: DHCP dinâmico” (p 672).

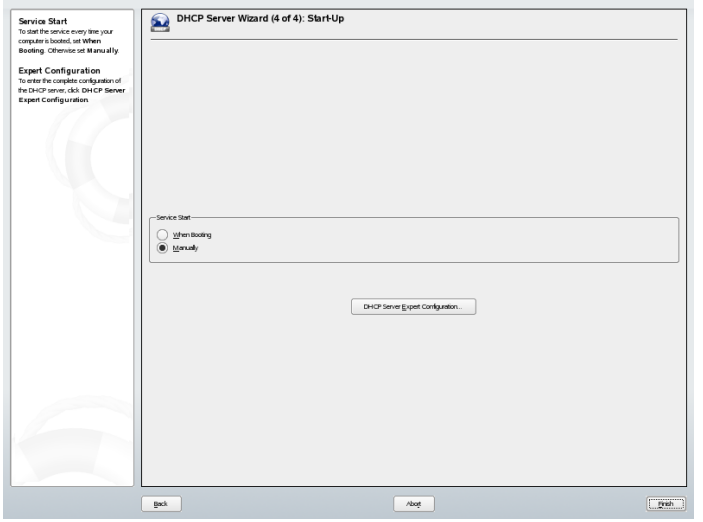
Figura 43.3 *Servidor DHCP: DHCP dinâmico*


IP Address Range
Here, set the First IP Address and the Last IP Address to lease to the clients. These addresses must have the same netmask. For instance, 192.168.1.1 and 192.168.1.64
Lease Time
Here, set the Default lease time for the current IP address range, which sets the optimal IP refreshing time for clients.
Maximum (optional value) sets the maximum time period for which this IP is blocked for the client on the DHCP server.
DHCP Server Wizard (3 of 4): Dynamic DHCP
IP Address Range
Current Network
10.20.0.0
Current Netmask
255.255.240.0
First IP Address
10.20.0.5
Last IP Address
10.20.0.255
Lease Time
Default
4
Hours
Maximum
2
Days
Back
Abort
Next

Concluindo a configuração e definindo o modo de início

Depois da terceira parte do assistente de configuração, uma última caixa de diálogo é mostrada, na qual você pode definir como o servidor DHCP deve ser inicializado. Aqui, especifique se o servidor DHCP deve iniciar automaticamente quando o sistema for inicializado ou iniciar manualmente (por exemplo, para fins de teste) quando necessário. Clique em *Concluir* para concluir a configuração do servidor. Consulte a Figura 43.4, “Servidor DHCP: Inicialização” (p 673).

Figura 43.4 *Servidor DHCP: Inicialização*


Service Start
To start the service every time your computer is booted, set When Booting. Otherwise set Manually.
Expert Configuration
To enter the complete configuration of the DHCP server, click DHCP Server Expert Configuration.
DHCP Server Wizard (4 of 4): Start-Up
Service Start
When Booting
Manually
DHCP Server Expert Configuration...
Back
Abort
Finish

43.2 Pacotes de software DHCP

Tanto um servidor DHCP quanto clientes DHCP estão disponíveis para o SUSE Linux. O servidor DHCP disponível é o dhcpd (publicado pelo Internet Software Consortium). No lado do cliente, escolha entre dois programas clientes DHCP: dhclient (também do ISC) e daemon cliente do DHCP no pacote `dhcpcd`.

O SUSE Linux instala o dhcpcd por padrão. O programa é muito fácil de manusear e é iniciado automaticamente em cada inicialização do sistema para monitorar um servidor DHCP. Ele não precisa de um arquivo de configuração para fazer seu trabalho e funciona assim que é instalado na maioria das configurações padrão. Em situações mais complexas, use o dhclient ISC, que é controlado por meio de um arquivo de configuração `/etc/dhclient.conf`.

43.3 O dhcpd do servidor DHCP

O núcleo de qualquer sistema DHCP é o daemon do protocolo de configuração do host dinâmico. Esse servidor *aluga* endereços e observa como são usados, de acordo com

as configurações definidas no arquivo de configuração `/etc/dhcpd.conf`. Ao mudar os parâmetros e valores desse arquivo, um administrador de sistemas pode influenciar o comportamento do programa de várias formas. Observe o arquivo de amostra básica `/etc/dhcpd.conf` em Exemplo 43.1, “Arquivo de configuração /etc/dhcpd.conf” (p 674).

Exemplo 43.1 *Arquivo de configuração /etc/dhcpd.conf*

```
tempo de aluguel padr o 600;         # 10 minutos
tempo de aluguel m x 7200;            # 2 horas

opç o nome de domínio "cosmos.all";
opç o servidores de nomes de domínio 192.168.1.1, 192.168.1.2;
opç o endereço de broadcast 192.168.1.255;
opç o roteadores 192.168.1.254;
opç o m scara de sub-rede 255.255.255.0;

sub-rede 192.168.1.0 m scara de rede 255.255.255.0
 {
  intervalo 192.168.1.10 192.168.1.20;
  intervalo 192.168.1.100 192.168.1.200;
 }
```

Esse arquivo de configuração simples deve ser suficiente para que o servidor DHCP designe endereços IP à rede. Verifique se um ponto-e-vírgula foi inserido no final de cada linha, caso contrário, o dhcpd não será iniciado.

O arquivo de amostra anterior pode ser dividido em três seções. A primeira define quantos segundos um endereço IP é alugado para um cliente que o solicitou por padrão (`tempo de aluguel padr o`) antes de solicitar uma renovação. Essa parte também inclui uma declaração do período máximo em que uma máquina pode manter um endereço IP designado pelo servidor DHCP sem solicitar uma renovação (`max-lease-time`).

Na segunda parte, alguns parâmetros de rede básicos são definidos em um nível global:

- A linha `option domain-name` define o domínio padrão da sua rede.
- Com a entrada `option domain-name-servers`, especifique até três valores para os servidores DNS usados para resolver endereços IP em nomes de host e vice-versa. Preferencialmente, configure um servidor de nomes em sua máquina ou em qualquer outra da rede antes de configurar o DHCP. Esse servidor de nomes deve também definir um nome de host para cada endereço dinâmico e vice-versa.

Para aprender a configurar o seu próprio servidor de nomes, leia o Capítulo 40, *Domain Name System (Sistema de Nomes de Domínio)* (p 633).

- A linha `option broadcast-address` define o endereço de broadcast a ser usado pelo cliente solicitante.
- Com `option routers`, informe ao servidor o destino de pacotes de dados que não podem ser enviados para um host da rede local (de acordo com o endereço de host de origem e de destino e da máscara de sub-rede fornecidos). Na maioria dos casos, especialmente em redes menores, esse roteador é idêntico ao gateway da Internet.
- Com `option subnet-mask`, especifique a máscara de rede designada a clientes.

A última seção do arquivo existe para definir uma rede, incluindo uma máscara de sub-rede. Para concluir, especifique a faixa de endereços que o daemon do DHCP deve usar para designar endereços IP a clientes interessados. Neste exemplo, os clientes podem receber qualquer endereço entre `192.168.1.10` e `192.168.1.20`, assim como `192.168.1.100` e `192.168.1.200`.

Depois de editar essas poucas linhas, você deverá conseguir ativar o daemon do DHCP com o comando `rcdhcpd start`. Ele poderá ser usado imediatamente. Use o comando `rcdhcpd check-syntax` para executar uma rápida verificação de sintaxe. Se houver problemas inesperados em sua configuração (o servidor for interrompido com um erro ou não retornar `done` na inicialização), você deverá descobrir o que aconteceu de errado, procurando informações no registro do sistema principal `/var/log/messages` ou no console 10 (Ctrl + Alt + F10).

Em um sistema SUSE Linux padrão, o daemon do DHCP é iniciado em um ambiente chroot por razões de segurança. Os arquivos de configuração precisam ser copiados para o ambiente chroot para que o daemon possa localizá-los. Normalmente, não é preciso se preocupar com isso, pois o comando `rcdhcpd start` copia automaticamente os arquivos.

43.3.1 Clientes com endereços IP fixos

Conforme mencionado antes, o DHCP também pode ser usado para designar um endereço estático predefinido a um cliente específico para cada solicitação. Endereços designados explicitamente sempre têm prioridade sobre endereços dinâmicos do pool.

Além disso, um endereço estático nunca expira da mesma forma que o dinâmico, por exemplo, se não houver endereços suficientes disponíveis, o servidor precisará redistribuí-los entre clientes.

Para identificar um cliente configurado com um endereço *estático*, o dhcpd usa o endereço de hardware, que é um código numérico fixo, globalmente exclusivo, consistindo em seis pares de octetos para a identificação de todos os dispositivos da rede (por exemplo, `00:00:45:12:EE:F4`). Se as respectivas linhas, como as que estão no Exemplo 43.2, “Adições ao arquivo de configuração” (p 676), forem adicionadas ao arquivo de configuração do Exemplo 43.1, “Arquivo de configuração /etc/dhcpd.conf” (p 674), o daemon do DHCP sempre designará o mesmo conjunto de dados ao cliente correspondente em qualquer circunstância.

Exemplo 43.2 *Adições ao arquivo de configuração*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

O nome do respectivo cliente (`host` *`nome do host`*, aqui `earth`) é digitado na primeira linha e o endereço MAC na segunda linha. Em hosts Linux, esse endereço pode ser determinado com o comando `ifstatus`, seguido do dispositivo de rede (por exemplo, `eth0`). Se necessário, ative a placa de rede primeiro com `ifup eth0`. A saída deve conter algo como

```
link/ether 00:00:45:12:EE:F4
```

No exemplo anterior, um cliente com uma placa de rede, cujo endereço MAC é `00:00:45:12:EE:F4`, adquire o endereço IP `192.168.1.21` e o nome de host earth automaticamente. O tipo de hardware a ser inserido é `ethernet` em quase todos os casos, embora `token-ring`, utilizado freqüentemente em sistemas IBM, também seja suportado.

43.3.2 Versão SUSE Linux

Para aprimorar a segurança, a versão SUSE do servidor DHCP do ISC vem com o patch não-raiz/chroot de Ari Edelkind aplicado. Isso permite que o dhcpd seja executado com o ID de usuário `nobody` e em um ambiente chroot (`/var/lib/dhcp`). Para que isso seja possível, o arquivo de configuração `dhcpd.conf` precisa estar localizado em

/var/lib/dhcp/etc. O script init copia automaticamente o arquivo para esse diretório na inicialização.

Controle o comportamento do servidor em relação a esse recurso, por meio de entradas no arquivo /etc/sysconfig/dhcpd. Para executar o dhcpd sem o ambiente chroot, configure a variável DHCPD_RUN_CHROOTED em /etc/sysconfig/dhcpd para "não".

Para permitir que o dhcpd resolva nomes de host, mesmo de dentro do ambiente chroot, alguns outros arquivos de configuração também precisam ser copiados:

- /etc/localtime
- /etc/host.conf
- /etc/hosts
- /etc/resolv.conf

Esses arquivos são copiados para /var/lib/dhcp/etc/ quando o script init é iniciado. Faça as mudanças necessárias nessas cópias, caso sejam modificadas dinamicamente por scripts como /etc/ppp/ip-up. Entretanto, você não precisará se preocupar com isso se o arquivo de configuração especificar somente endereços IP (em vez de nomes de host).

Se a configuração incluir arquivos adicionais que devem ser copiados para o ambiente chroot, especifique-os na variável DHCPD_CONF_INCLUDE_FILES do arquivo /etc/sysconfig/dhcpd. Para garantir que o recurso de registro DHCP continue funcionando, mesmo depois de uma reinicialização do daemon do syslog, é necessário adicionar a opção "-a /var/lib/dhcp/dev/log" em SYSLOGD_PARAMS do arquivo /etc/sysconfig/syslog.

43.4 Para obter mais informações

Há mais informações disponíveis sobre o DHCP no site do *Internet Software Consortium* (http://www.isc.org/products/DHCP/). Também é possível encontrar informações nas páginas de manual do dhcpd, dhcpd.conf, dhcpd.leases e dhcp-options.

44 Sincronização de horário com xntp

O mecanismo NTP (network time protocol) é um protocolo para sincronizar a hora do sistema na rede. Primeiro, uma máquina pode obter a hora de um servidor, que é uma fonte de tempo confiável. Segundo, a máquina pode agir como uma fonte de horário para outros computadores na rede. O objetivo é duplo—manter o tempo absoluto e a sincronização do horário do sistema de todas as máquinas na rede.

Manter uma hora de sistema exata é importante em várias situações. O relógio do hardware interno (BIOS) não atende aos requisitos de aplicativos como bancos de dados. A correção manual da hora do sistema levaria a problemas severos pois, por exemplo, um pulo inverso pode causar o mau funcionamento de aplicativos críticos. Em uma rede, em geral é necessário sincronizar a hora do sistema em todas as máquinas, mas o ajuste de hora manual não é uma boa abordagem. O xntp fornece um mecanismo para resolver esses problemas. Ele ajusta continuamente a hora do sistema com a ajuda de servidores de horário confiáveis na rede. Ele habilita também o gerenciamento de relógios de referência local como relógios controlados pelo rádio.

44.1 Configurando um cliente NTP com YaST

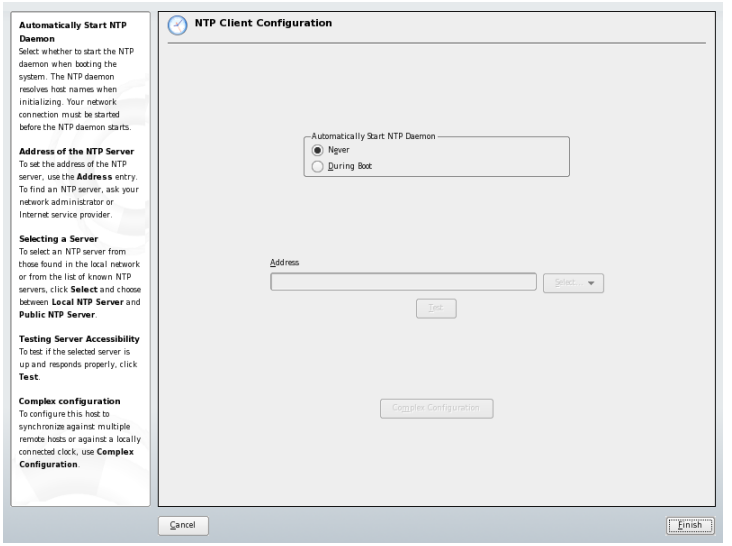
O xntp está predefinido para usar o relógio do computador local como referência de horário. Usar o relógio (BIOS), porém, serve somente como uma alternativa caso não haja uma fonte de horário de precisão maior disponível. O SUSE Linux facilita a configuração de um cliente NTP com YaST. Use a configuração rápida ou complexa

em clientes que não executam o SUSEfirewall porque esses clientes pertencem a uma intranet protegida. Ambas estão descritas no seguinte.

44.1.1 Configuração de cliente NTP rápida

A configuração de cliente NTP fácil (*Serviços de Rede → Cliente NTP*) consiste em duas caixas de diálogo. Defina o modo de inicialização do xntpd e do servidor para consultar a primeira caixa de diálogo. Para iniciar o xntpd automaticamente quando o sistema for inicializado, clique em *Durante a Inicialização*. Em seguida, clique em *Selecionar* para acessar uma segunda caixa de diálogo na qual é possível selecionar um servidor de horário adequado para a rede.

Figura 44.1 *YaST: Configurando um cliente NTP*


Automatically Start NTP Daemon
Select whether to start the NTP daemon when booting the system. The NTP daemon resolves host names when initializing. Your network connection must be started before the NTP daemon starts.
Address of the NTP Server
To set the address of the NTP server, use the Address entry. To find an NTP server, ask your network administrator or Internet service provider.
Selecting a Server
To select an NTP server from those found in the local network or from the list of known NTP servers, click Select and choose between Local NTP Server and Public NTP Server.
Testing Server Accessibility
To test if the selected server is up and responds properly, click Test.
Complex configuration
To configure this host to synchronize against multiple remote hosts or against a locally connected clock, use Complex Configuration.
NTP Client Configuration
Automatically Start NTP Daemon
Never
During Boot
Address
Select...
Test
Complex Configuration
Cancel
Finish

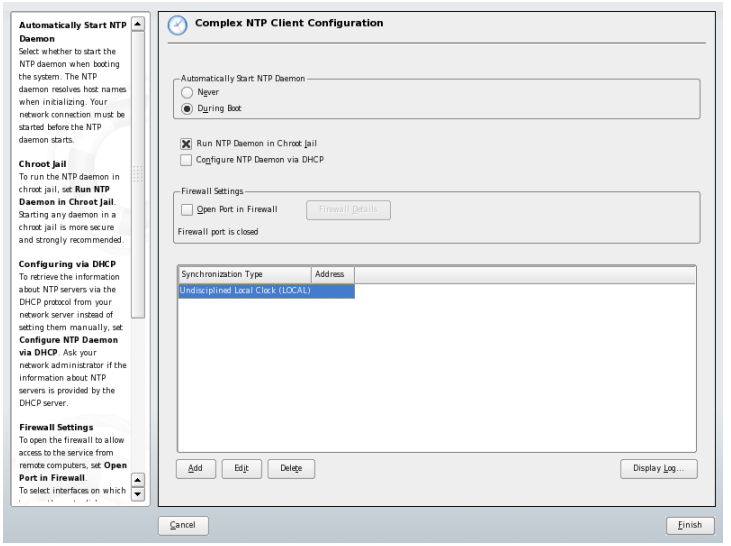
Na caixa de diálogo de servidor detalhada, determine se você implementará a sincronização de horário usando um servidor de horário a partir da rede local (*Servidor NTP Local*) ou um servidor de horário baseado na Internet que lida com o seu fuso horário (*Servidor NTP Público*). Para um servidor de horário local, clique em *Busca* para iniciar uma consulta SLP por servidores de horário disponíveis na sua rede. Selecione o servidor de horário mais adequado a partir da lista de resultados de pesquisa e saia da caixa de diálogo com *OK*. Para um servidor de horário público, selecione o país (fuso horário) e um servidor adequado da lista sob *Servidor NTP Público*, em

seguida, saia da caixa de diálogo com *OK*. Na caixa de diálogo principal, teste a disponibilidade do servidor selecionado com *Testar* e saia da caixa de diálogo com *Concluir*.

44.1.2 Configuração de Cliente NTP Complexa

A configuração complexa de um cliente NTP pode ser acessada sob *Configuração Complexa* na caixa de diálogo principal do módulo *Cliente NTP*, mostrado em Figura 44.1, “YaST: Configurando um cliente NTP” (p 680), após selecionar o modo de inicialização conforme descrito na configuração rápida.

Figura 44.2 *YaST: Configuração de Cliente NTP Complexa*


Automatically Start NTP Daemon
Select whether to start the NTP daemon when booting the system. The NTP daemon resolves host names when initializing. Your network connection must be started before the NTP daemon starts.
Chroot Jail
To run the NTP daemon in chroot jail, set Run NTP Daemon in Chroot Jail. Starting any daemon in a chroot jail is more secure and strongly recommended.
Configuring via DHCP
To retrieve the information about NTP servers via the DHCP protocol from your network server instead of setting them manually, set Configure NTP Daemon via DHCP. Ask your network administrator if the information about NTP servers is provided by the DHCP server.
Firewall Settings
To open the firewall to allow access to the service from remote computers, set Open Port in Firewall.
Complex NTP Client Configuration
Automatically Start NTP Daemon
Never
During Boot
Run NTP Daemon in Chroot Jail
Configure NTP Daemon via DHCP
Firewall Settings
Open Port in Firewall
Firewall Details...
Firewall port is closed
Synchronization Type
Address
Undisciplined Local Clock (LOCAL)
Add
Edit
Delete
Display Log...
Cancel
Finish

Em *Configuração de Cliente NTP Complexa*, determine se xntpd deve ser iniciado em uma cadeia chroot. Isso aumenta a segurança caso ocorra um ataque em xntpd, pois isso evita que o invasor comprometa todo o sistema. *Configurar o Daemon NTP via DHCP* configura o cliente NTP para obter uma lista dos servidores NTP disponíveis na rede via DHCP.

Os servidores e outras fontes de horário para cliente a serem consultados estão listados na parte inferior. Modifique esta lista conforme necessário com *Adicionar*, *Editar* e *Apagar*. *Exibir Registro* fornece a possibilidade de exibir os arquivos de registro do seu cliente.

Clique em *Adicionar* para adicionar uma nova fonte de informação de horário. Na caixa de diálogo seguinte, selecione o tipo de fonte com a qual a sincronização de horário deve ser realizada. As seguintes opções estão disponíveis:

Servidor
Outra caixa de diálogo permite selecionar um servidor NTP (conforme descrito em Seção 44.1.1, “Configuração de cliente NTP rápida” (p 680)). Ative *Usar para Sincronização Inicial* para acionar a sincronização da informação de horário entre o servidor e o cliente quando o sistema é inicializado. Um campo de entrada permite especificar opções adicionais para xntpd. Consulte `/usr/share/doc/packages/xntp-doc` (parte do pacote `xntp-doc`) para obter informações detalhadas.

Parceiro
Um parceiro é uma máquina à qual uma relação simétrica é estabelecida: ele age como um servidor de horário e como cliente. Para usar um parceiro na mesma rede em vez de um servidor, insira o endereço do sistema. O restante da caixa de diálogo é igual à caixa de diálogo *Servidor*.

Relógio controlado pelo rádio
Para usar um relógio controlado pelo rádio no seu sistema para a sincronização de horário, insira o tipo de relógio, o número da unidade, o nome do dispositivo e outras opções nesta caixa de diálogo. Clique em *Calibração do Driver* para ajustar o driver. Informações detalhadas sobre a operação de um relógio controlado por rádio local estão disponíveis em `/usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Transmissão de saída
Consultas e informações sobre horário também podem ser transmitidas na rede. Nesta caixa de diáligo, insira o endereço ao qual estas transmissões devem ser enviadas. Não ative a transmissão a menos que você tenha uma fonte de horário confiável como um relógio controlado por rádio.

Transmissão de entrada
Se você deseja que o seu cliente receba suas informações através de transmissão, insira o endereço do qual os respectivos pacotes devem ser aceitos nestes campos.

44.2 Configurando o xntp na rede

A forma mais fácil de usar um servidor de horário na rede é definir parâmetros de servidor. Por exemplo, se um servidor de horário chamado `ntp.example.com` for alcançável a partir da rede, adicione seu nome ao arquivo `/etc/ntp.conf` adicionando a linha `server ntp.example.com`. Para adicionar mais servidores de horário, insira linhas adicionais com o servidor de palavras-chave. Após inicializar o xntpd com o comando `rcxntpd start`, leva aproximadamente uma hora até que o horário esteja estabilizado e o arquivo de registro para corrigir o relógio do computador local seja criado. Com o arquivo de registro, o erro sistemático do relógio do hardware pode ser computado assim que o computador for ligado. A correção é usada imediatamente, resultando em uma estabilidade maior do horário do sistema.

Há duas maneiras possíveis de usar o mecanismo NTP como um cliente: Primeiro, o cliente pode consultar o horário a partir de um servidor conhecido em intervalos regulares. Com vários clientes, esta abordagem pode causar uma carga alta no servidor. Segundo, o cliente pode esperar por transmissões de NTP enviadas por servidores de horário de transmissão na rede. Esta abordagem tem a desvantagem de que a qualidade do servidor é desconhecida e um servidor transmitindo a informação errada pode causar problemas graves.

Se o horário for obtido através de uma transmissão você não precisa do nome do servidor. Neste caso, insira a linha `broadcastclient` no arquivo de configuração `/etc/ntp.conf`. Para usar um ou mais servidores de horário conhecidos exclusivamente, insira seus nomes na linha iniciando com `servers`.

44.3 Configurando um relógio de referência local

O pacote de software xntp contém drivers para conectar relógios de referência local. Uma lista de relógios suportados está disponível no pacote `xntp-doc` no arquivo `/usr/share/doc/packages/xntp-doc/html/refclock.htm`. Cada driver

está associado a um número. No xntp, a configuração real ocorre através de pseudo IPs. Os relógios são inseridos no arquivo `/etc/ntp.conf` como se existissem na rede. Para este propósito, endereços IP especiais são atribuídos a eles na forma `127.127.t.u`. Aqui, `t` representa o tipo de relógio e determina o driver a ser usado e `u` para unidade, que determina a interface usada.

Normalmente, os drivers individuais têm parâmetros especiais que descrevem detalhes de configuração. O arquivo `/usr/share/doc/packages/xntp-doc/html/driverNN.htm` (onde `NN` é o número do driver) fornece informações sobre o tipo específico de relógio. Por exemplo, o relógio "type 8" (relógio controlado por rádio na interface serial) exige um modo adicional que especifica o relógio de forma mais precisa. O módulo de recebimento Conrad DCF77, por exemplo, tem o mode 5. Para usar este relógio como referência preferida, especifique a palavra-chave `prefer`. A linha do `servidor` completa para um módulo de recebimento Conrad DCF77 seria:

```
server 127.127.8.0 mode 5 prefer
```

Outros relógios seguem o mesmo padrão. Seguindo a instalação do pacote `xntp-doc`, a documentação para o xntp está disponível no diretório `/usr/share/doc/packages/xntp-doc/html`. O arquivo `/usr/share/doc/packages/xntp-doc/html/refclock.htm` fornece links para as páginas do driver descrevendo os parâmetros do driver.

LDAP—Um serviço de diretório 45

O LDAP é um conjunto de protocolos criado para acessar e manter diretórios de informações. O LDAP pode ser usado para vários propósitos, como gerenciamento de grupos e usuários, gerenciamento de configuração de sistema ou gerenciamento de endereços. Este capítulo fornece uma compreensão básica sobre como o OpenLDAP funciona e como gerenciar dados do LDAP com o YaST. Embora haja várias implementações do protocolo LDAP, este capítulo concentra-se inteiramente na implementação do OpenLDAP.

É crucial em um ambiente de rede manter informações importantes estruturadas e rapidamente disponíveis. Isso pode ser realizado com um serviço de diretório que, como as páginas amarelas comuns, mantém informações disponíveis em uma forma bem estruturada e rapidamente pesquisável.

No caso ideal, um servidor central mantém os dados em um diretório e os distribui a todos os clientes usando um determinado protocolo. Os dados são estruturados de forma a permitir que uma ampla variedades de aplicativos os acessem. Desta forma, não é necessário para cada ferramenta de calendário e cliente de e-mail manter seu próprio banco de dados—um repositório central pode ser acessado em vez disso. Isso reduz bastante o esforço de administração para as informações. O uso de um protocolo padronizado e aberto como o LDAP garante que muitos aplicativos de cliente diferentes possam acessar tais informações.

Um diretório neste contexto é um tipo de banco de dados otimizado para pesquisa e leitura rápida e efetiva:

- Para possibilitar vários acessos de leitura (simultâneos), o acesso de gravação está limitado a um pequeno número de atualizações pelo administrador. Bancos de

dados convencionais são otimizados para aceitar o mais amplo volume de dados possível em um período curto de tempo.

- Como acessos de gravação só podem ser executados de forma restrita, um serviço de diretório é usado para administrar, em sua maioria, informações estáticas, sem alterações. Dados em um banco de dados convencional normalmente são alterados com freqüência (dados *dinâmicos*). Números de telefone em um diretório de empresa não são alterados com tanta freqüência como, por exemplo, os números administrados em contabilidade.

- Quando dados estáticos são administrados, atualizações dos conjuntos de dados existentes são muito raras. Ao trabalhar com dados dinâmicos, especialmente relativos a conjuntos de dados como contas de banco ou contabilidade, a consistência dos dados é de importância fundamental. Se um valor deve ser subtraído de um local para ser adicionado a outro, ambas as operações devem ocorrer simultaneamente, em uma *transação*, para garantir o equilíbrio sobre o estoque de dados. Bancos de dados suportam estas transações. Diretórios não suportam estas transações. Inconsistências de curto prazo dos dados são aceitáveis em diretórios.

O design de um serviço de diretório como o LDAP não é criado para suportar mecanismos de consulta ou atualização complexa. Todos os aplicativos acessando este serviço devem obter acesso de forma rápida e fácil.

Vários serviços de diretório existiram previamente e ainda existem no Unix e fora dele. Novell NDS, Microsoft ADS, Banyan's Street Talk e o OSI standard X.500 são apenas alguns exemplos. O LDAP foi originalmente planejado como uma versão menor do DAP, o protocolo de acesso de diretório, que foi desenvolvido para acessar o X.500. O padrão do X.500 regula a organização hierárquica de entradas de diretório.

O LDAP é uma versão menor do DAP. Sem perder a hierarquia de entrada do X.500, beneficie-se das capacidades de plataforma cruzada do LDAP e salve recursos. O uso de TCP/IP facilita o estabelecimento de interfaces entre um aplicativo de acoplagem e o serviço LDAP.

O LDAP, enquanto isso, evoluiu e é usado cada vez mais como uma solução independente sem o suporte do X.500. O LDAP suporta *referências* com o LDAPv3 (a versão de protocolo no pacote `openldap2`), possibilitando ter bancos de dados distribuídos. O uso de SASL (autenticação simples e camada de segurança) também é novo.

O LDAP não está limitado a consultar dados dos servidores X.500, como foi planejado originalmente. Há um servidor de código aberto slapd, que pode armazenar informações de objetos em um banco de dados local. Há também uma extensão chamada slurpd, que é responsável por replicar vários servidores LDAP.

O pacote `openldap2` consiste em:

slapd
Um servidor LDAPv3 independente que administra informações de objeto em um banco de dados baseado em BerkeleyDB.

slurpd
Este programa habilita a replicação de modificações aos dados no servidor LDAP local para outros servidores LDAP instalados na rede.

ferramentas adicionais para manutenção do sistema
`slapcat`, `slapadd`, `slapindex`

45.1 LDAP versus NIS

O administrador do sistema Unix tradicionalmente usa o serviço NIS para resolução de nomes e distribuição de dados em uma rede. Os dados de configuração contidos nos arquivos em `/etc` e os diretórios `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` e `services` são distribuídos por clientes em toda a rede. Estes arquivos podem ser mantidos sem maior esforço pois são arquivos de texto simples. O tratamento de grandes quantidades de dados, porém, torna-se mais difícil devido a estrutura não existente. O NIS é criado somente para plataformas Unix, o que torna o seu uso como administrador de dados central em uma rede heterogênea impossível.

Ao contrário do NIS, o serviço LDAP não está restrito a redes Unix puras. Servidores do Windows (do 2000) suportam o LDAP como um serviço de diretório. A Novell também oferece um serviço LDAP. Tarefas de aplicativo mencionadas acima são suportadas adicionalmente em sistemas não-Unix.

O princípio LDAP pode ser aplicado a qualquer estrutura de dados que deva ser administrado de forma central. Alguns exemplos de aplicativos são:

- Utilização como substituto do serviço NIS

- Rota de correio (postfix, sendmail)
- Blocos de endereços para clientes de correio, como Mozilla, Evolution e Outlook
- Administração de descrições de zona para um servidor de nomes BIND9
- Autenticação do usuário com Samba em redes heterogêneas

Esta lista pode ser estendida pois o LDAP é extensível, ao contrário do NIS. A estrutura hierárquica claramente definida dos dados facilita a administração de grandes quantidades de dados, pois pode ser pesquisada de forma melhor.

45.2 Estrutura de uma árvore de diretórios LDAP

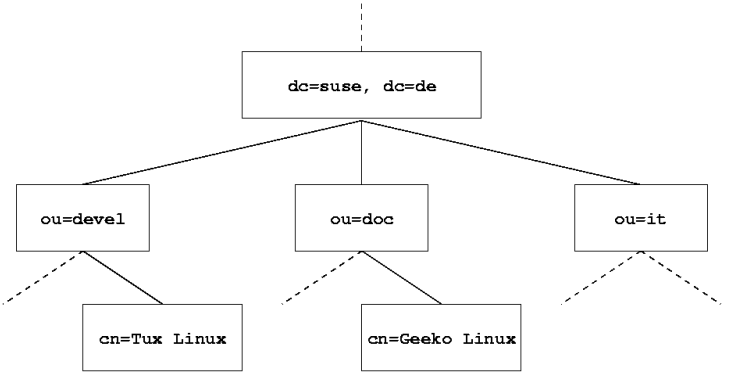
Um diretório LDAP tem uma estrutura de árvores. Todas as entradas (chamadas objetos) do diretório têm uma posição definida nesta hierarquia. Esta hierarquia é chamada de *árvore de informação de diretórios* (DIT). O caminho completo à entrada desejada, que a identifica de forma clara, é chamado *nome distinto* ou DN. Um único nó no caminho para esta entrada é chamado *nome distinto relativo* ou RDN. Objetos podem geralmente ser atribuídos a um ou dois tipos possíveis:

container
: Estes objetos podem conter outros objetos. Tais classes de objetos são `root` (o elemento root da árvore de diretórios, que não existe realmente), `c` (país) `ou` (unidade organizacional) e `dc` (componente do domínio). Este modelo é comparável aos diretórios (pastas) em um sistema de arquivos.

folha
: Estes objetos estão no final de uma ramificação e não têm objetos subordinados. Exemplos: `person`, `InetOrgPerson` ou `groupofNames`.

O topo da hierarquia de diretório tem um elemento root `root`. Isso pode conter `c` (país), `dc` (componente de domínio) ou `o` (organização) como elementos subordinados. As relações em uma árvore de diretórios LDAP tornam-se mais evidentes no exemplo seguinte, mostrado em Figura 45.1, “Estrutura de um diretório LDAP” (p 689).

Figura 45.1 *Estrutura de um diretório LDAP*



O diagrama completo compreende uma árvore de informações de diretório ficcional. As entradas em três níveis estão apresentadas. Cada entrada corresponde a uma caixa na figura. O *nome distinto* válido e completo para o funcionário SUSE ficcional `Geeko Linux`, neste caso é `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Ele é composto através da adição do RDN `cn=Geeko Linux` ao DN da entrada anterior `ou=doc,dc=suse,dc=de`.

A determinação global dos tipos de objetos que devem ser armazenados no DIT é realizada segundo um *esquema*. O tipo de um objeto é determinado pela *classe de objeto*. A classe de objeto determina quais atributos podem ou devem ser atribuídos ao objeto em questão. Portanto, um esquema deve conter definições de todos atributos e classes de objetos usados no cenário do aplicativo desejado. Há alguns esquemas comuns (consulte RFC 2252 e 2256). Porém, é possível criar esquemas personalizados ou usar vários esquemas complementando um ao outro se isso for exigido pelo ambiente no qual o servidor LDAP deve operar.

Tabela 45.1, “Atributos e classes de objeto usados comumente” (p 690) oferece uma pequena visão geral das classes de objeto de `core.schema` e `inetorgperson.schema` usadas no exemplo, incluindo atributos necessários e valores de atributos válidos.

Tabela 45.1 *Atributos e classes de objeto usados comumente*

Classe de objeto	Significado	Entrada de exemplo	Atributos compulsórios
dcObject	*domainComponent* (nomeie componentes do domínio)	suse	dc
organizationalUnit	*organizationalUnit* (unidade organizacional)	doc	ou
inetOrgPerson	*inetOrgPerson* (dados relativos a pessoas para a intranet ou Internet)	Geeko Linux	sn e cn

Exemplo 45.1, “Exemplo de schema.core ” (p 690) mostra um exemplo de uma diretiva de esquemas com explicações (numeração de linha para motivos explanatórios).

Exemplo 45.1 *Exemplo de schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: unidade organizacional à qual este objeto pertence'
#3        nome SUP )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5        DESC 'RFC2256: an organizational unit'
#6        SUP top STRUCTURAL
#7        MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
    $ x121Address $ registeredAddress $ destinationIndicator
    $ preferredDeliveryMethod $ telexNumber
    $ teletexTerminalIdentifier $ telephoneNumber
    $ internationaliSDNNumber $ facsimileTelephoneNumber
    $ street $ postOfficeBox $ postalCode $ postalAddress
    $ physicalDeliveryOfficeName
    $ st $ l $ description) )
...
```

O tipo de atributo `organizationalUnitName` e a classe de objeto correspondente `organizationalUnit` servem como um exemplo aqui. A linha 1 apresenta o nome do atributo, seu OID exclusivo (*identificador de objeto*) (numérico) e a abreviação do atributo.

A linha 2 fornece uma descrição breve do atributo com `DESC`. O RFC correspondente na qual a definição é baseada também é mencionado aqui. `SUP` na linha 3 indica um tipo de atributo super ordenado ao qual este atributo pertence.

A definição da classe de objeto `organizationalUnit` começa na linha 4, como na definição do atributo, com um OID e o nome da classe de objeto. A linha 5 apresenta uma breve descrição da classe de objeto. A linha 6, com esta entrada `SUP top`, indica que esta classe de objeto não está subordinada a outra classe de objeto. A linha 7, começando com `MUST`, lista todos os tipos de atributo que *devem* ser usados em conjunto com um objeto do tipo `organizationalUnit`. A linha 8, começando com `MAY`, lista todos os tipos de atributos que são permitidos em conjunto com esta classe de objeto.

Uma boa introdução para o uso de esquemas pode ser encontrada na documentação de OpenLDAP. Quando instalada, encontre-a em `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

45.3 Configuração do servidor com slapd.conf

O seu sistema instalado contém um arquivo de configuração completo para o seu servidor LDAP em `/etc/openldap/slapd.conf`. As únicas entradas estão descritas brevemente aqui e os ajustes necessários são explicados. Entradas com prefixo de hash (#) são inativas. Este caractere de comentário deve ser removido para ativá-las.

45.3.1 Diretivas globais em slapd.conf

Exemplo 45.2 *slapd.conf: Incluir diretiva para esquemas*

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

A primeira diretiva em `slapd.conf`, mostrada em Exemplo 45.2, “slapd.conf: Incluir diretiva para esquemas” (p 691), specifica o esquema através do qual o diretório LDAP é organizado. A entrada `core.schema` é compulsória. Esquemas necessários adicionais

estão anexados a esta diretiva. Informações podem ser encontradas na documentação do OpenLDAP incluída.

Exemplo 45.3 *slapd.conf: pidfile e argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Estes dois arquivos contêm o PID (ID de processo) e alguns dos argumentos com os quais o processo `slapd` é iniciado. Não há necessidade para modificações aqui.

Exemplo 45.4 *slapd.conf: Controle de acesso*

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
              by users read
              by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

Exemplo 45.4, “slapd.conf: Controle de acesso” (p 692) é o exemplo de `slapd.conf` que regula as permissões de acesso para o diretório LDAP no servidor. As configurações realizadas aqui na seção global de `slapd.conf` são válidas desde que nenhuma regra de acesso personalizada seja declarada na seção específica ao banco de dados. Estas devem sobrescrever as declarações globais. Conforme apresentado aqui, todos os usuários têm acesso de leitura ao diretório, mas somente o administrador (`rootdn`) pode gravar para este diretório. O regulamento de controle de acesso no LDAP é um processo altamente complexo. As dicas a seguir podem ajudar:

- Toda regra de acesso tem a seguinte estrutura:

  ```
  acesso a <what> por <who> <access>
  ```

- *`what`* é um marcador para o objeto ou atributo ao qual acesso é concedido. Ramificações de diretório individuais podem ser protegidas explicitamente com regras separadas. Também é possível processar regiões da árvore de diretórios com uma única regra usando expressões regulares. `slapd` avalia todas as regras na ordem em que elas estão listadas no arquivo de configuração. Mais regras gerais

devem estar listadas após outras mais específicas—a primeira regra `slapd` considerada válida é avaliada e todas as entradas seguintes são ignoradas.

- *`who`* determina a quem deve ser concedido acesso às áreas determinadas com *`what`*. Expressões regulares podem ser usadas. `slapd` novamente anula a avaliação de `who` após a primeira correspondência, por isso regras mais específicas devem ser listadas antes das mais gerais. As entradas mostradas em Tabela 45.2, “Grupos de usuários e suas concessões de acesso” (p 693) são possíveis.

Tabela 45.2 *Grupos de usuários e suas concessões de acesso*

Tag	Escopo
`*`	Todos os usuários sem exceção
`anônimos`	Usuários (“anônimos”) não autenticados
`usu rios`	Usuários autenticados
`próprio`	Usuários conectados com o objeto de destino
`dn.regex=<regex>`	Todos os usuários que correspondem à expressão regular

- *`acesso`* especifica o tipo de acesso. Use as opções listadas em Tabela 45.3, “Tipos de acesso” (p 693).

Tabela 45.3 *Tipos de acesso*

Tag	Escopo do acesso
`nenhum`	Sem acesso
`autenticaç o`	Para entrar em contato com o servidor
`comparar`	Para objetos para acesso de comparação
`busca`	Para a utilização de filtros de busca

Tag	Escopo do acesso
`ler`	Acesso de leitura
`gravar`	Acesso de gravação

`slapd` compara o direito de acesso solicitado pelo cliente com os concedidos em `slapd.conf`. Acesso é concedido ao cliente se as regras permitirem um direito igual ou maior do que o solicitado. Se o cliente solicitar direitos maiores do que os declarados nas regras, o acesso é negado.

Exemplo 45.5, “slapd.conf: Exemplo de controle de acesso” (p 694) mostra um exemplo de um simples controle de acesso que pode ser desenvolvido arbitrariamente usando expressões regulares.

Exemplo 45.5 *slapd.conf: Exemplo de controle de acesso*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
by user read
by * none
```

Esta regra declara que somente o seu respectivo administrador tem acesso de gravação a uma entrada `ou` individual. Todos os outros usuários autenticados têm acesso de leitura e o restante do mundo não tem acesso.

DICA: Estabelecendo regras de acesso

Se não houver `acesso a` uma regra ou nenhuma correspondência `por` diretiva, o acesso é negado. Somente direitos de acesso explicitamente declarados são concedidos. Se nenhuma regra for declarada, o princípio padrão é o acesso de gravação para o administrador e o acesso de leitura para o restante do mundo.

Encontre informações detalhadas e uma configuração de exemplo para direitos de acesso LDAP na documentação online do pacote `openldap2` instalado.

Fora a possibilidade de administrar permissões de acesso com o arquivo de configuração do servidor central (`slapd.conf`), não há informações de controle de acesso (ACI). A ACI permite o armazenamento das informações de acesso para objetos individuais na árvore LDAP. Este tipo de controle de acesso ainda não é comum e é considerado

experimental pelos desenvolvedores. Consulte http://www.openldap.org/faq/data/cache/758.html para obter informações.

45.3.2 Diretivas específicas de bancos de dados em slapd.conf

Exemplo 45.6 *slapd.conf: Diretivas específicas de bancos de dados*

```
database bdb
checkpoint      1024    5
cachesize       10000
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  Consulte slappasswd(8) e slapd.conf(5) para obter detalhes.
# O uso de autenticaç o forte é encorajado.
rootpw secret
# O diretório de banco de dados DEVE existir antes da execuç o de slapd E
# deve estar acessível somente pelas slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

O tipo de banco de dados, um banco de dados Berkeley neste caso, é determinado na primeira linha desta seção (consulte Exemplo 45.6, “slapd.conf: Diretivas específicas de bancos de dados” (p 695)). `checkpoint` determina a quantidade de dados (em kb) mantida no registro de transação antes que seja gravada no banco de dados real e o tempo (em minutos) entre as duas ações de gravação. `cachesize` define o número de objetos mantidos no cache do banco de dados. `suffix` determina por qual parte da árvore LDAP este servidor deve ser responsável. O `rootdn` seguinte determina quem possui direitos de administrador para este servidor. O usuário declarado aqui não precisa ter uma entrada LDAP ou existir como um usuário regular. A senha do administrador é definida com `rootpw`. Em vez de usar `secret` aqui, é possível inserir o hash da senha do administrador criado por `slappasswd`. A diretiva `directory` indica o diretório (no sistema de arquivos) onde os diretórios de bancos de dados estão armazenados no servidor. A última diretiva, `index objectClass eq`, resulta na manutenção de um índice de todas as classes de objetos. Atributos para os quais os usuários pesquisam com freqüência podem ser adicionados aqui de acordo com a experiência. Regras de `acesso` personalizado definidas aqui para o banco de dados são usadas em vez de regras de `acesso` global.

45.3.3 Iniciando e interrompendo os servidores

Depois que o servidor LDAP estiver totalmente configurado e todas as entradas desejadas tiverem sido realizadas de acordo com o padrão descrito em Seção 45.4, “Tratamento de dados no diretório LDAP” (p 696), inicie o servidor LDAP como `root` inserindo `rcldap start`. Para interromper o servidor manualmente, insira o comando `rcldap stop`. Solicite o status do servidor LDAP em execução com o `rcldap status`.

O editor de níveis de execução YaST, descrito em Seção 28.2.3, “Configurando serviços do sistema (runlevel) com o YaST” (p 448), pode ser usado para que o servidor seja iniciado e interrompido automaticamente na inicialização e na pausa do sistema. Também é possível criar os links correspondentes aos scripts de início e interrupção com o comando `insserv` de um prompt de comando, conforme descrito na Seção 28.2.2, “Scripts Init” (p 444).

45.4 Tratamento de dados no diretório LDAP

O OpenLDAP oferece uma série de ferramentas para a administração de dados no diretório LDAP. A quatro ferramentas mais importantes para adicionar, apagar, pesquisar e modificar o estoque de dados são explicadas abaixo.

45.4.1 Inserindo dados em um diretório LDAP

Depois que a configuração do seu servidor LDAP em `/etc/openldap/lsapd.conf` estiver correta e pronta (ela apresenta entradas apropriadas para `suffix`, `directory`, `rootdn`, `rootpw` e `index`), continue a inserir registros. OpenLDAP oferece o comando `ldapadd` para esta tarefa. Se possível, adicione os objetos ao banco de dados em pacotes por razões práticas. O LDAP é capaz de processar o formato LDIF (formato intercambiável de dados LDAP) para isso. Um arquivo LDIF é um arquivo de texto simples que pode conter um número arbitrário de pares de atributo e valor. Consulte os arquivos de esquema declarados em `slapd.conf` para os atributos e as

classes de objeto disponíveis. O arquivo LDIF para criar uma estrutura bruta para o exemplo em Figura 45.1, “Estrutura de um diretório LDAP” (p 689) teria a mesma aparência que em Exemplo 45.7, “Exemplo de um arquivo LDIF” (p 697).

Exemplo 45.7 *Exemplo de um arquivo LDIF*

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

IMPORTANTE: Codificação de arquivos LDIF

O LDAP funciona com o UTF-8 (Unicode). Umlauts deve ser codificado corretamente. Use um editor que suporte UTF-8, como o Kate ou versões recentes de Emacs. De outra forma, evite umlauts e outros caracteres especiais ou use `recode` para registrar a entrada em UTF-8.

Salve o arquivo com o sufixo `.ldif`, em seguida, transmita-o ao servidor com o seguinte comando:

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

`-x` desliga a autenticação com o SASL neste caso. `-D` declara o usuário que chama a operação. O DN válido do administrador é inserido aqui como foi configurado em `slapd.conf`. No exemplo atual, há `cn=admin,dc=suse,dc=de`. `-W` evita a inserção de senha na linha de comando (em texto claro) e ativa um prompt de senha separado. Esta senha foi determinada previamente em `slapd.conf` com `rootpw`. `-f` transmite o nome de arquivo. Consulte os detalhes da execução de `ldapadd` em Exemplo 45.8, “ldapadd com example.ldif” (p 698).

Exemplo 45.8 *ldapadd com example.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif

Insira a senha do LDAP:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Os dados de usuário de indivíduos podem ser preparados em arquivos LDIF separados. Exemplo 45.9, “Dados LDIF para Tux” (p 698) adiciona `Tux` ao novo diretório LDAP.

Exemplo 45.9 *Dados LDIF para Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Um arquivo LDIF pode conter um número arbitrário de objetos. É possível transmitir ramificações de todo o diretório ao servidor de uma vez ou somente partes como mostrado no exemplo de objetos individuais. Se for necessário modificar alguns dados com freqüência, uma subdivisão de objetos únicos é recomendável.

45.4.2 Modificando dados no diretório LDAP

A ferramenta `ldapmodify` é fornecida para modificar o estoque de dados. A forma mais fácil de fazer isso é modificar o arquivo LDIF correspondente e, em seguida, transmitir este arquivo modificado ao servidor LDAP. Para alterar o número de telefone do colega Tux de `+49 1234 567-8` para `+49 1234 567-10`, edite o arquivo LDIF como em Exemplo 45.10, “Arquivo LDIF modificado tux.ldif” (p 699).

Exemplo 45.10 *Arquivo LDIF modificado tux.ldif*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importe o arquivo modificado no diretório LDAP com o seguinte comando:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Alternativamente, transmita os atributos para alterar diretamente para `ldapmodify`. O procedimento para isto está descrito abaixo:

1. Inicie `ldapmodify` e insira sua senha:

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W
   Enter LDAP password:
   ```

2. Insira as modificações e siga cuidadosamente a sintaxe na ordem apresentada abaixo:

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Informações detalhadas sobre `ldapmodify` e sua sintaxe podem ser encontradas na página de manual de ldapmodify(1).

45.4.3 Buscando ou lendo dados de um diretório LDAP

OpenLDAP fornece, com `ldapsearch`, uma ferramenta de linha de comando para pesquisar dados em um diretório LDAP e ler dados a partir dele. Uma consulta simples teria a seguinte sintaxe:

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

A opção `-b` determina a base de busca—a seção da árvore dentro da qual a busca deve ser executada. No caso atual, isto é `dc=suse,dc=de`. Para realizar uma busca mais detalhada em subseções específicas do diretório LDAP (por exemplo, somente no

departamento `devel`), transmita esta seção para `ldapsearch` com `-b`. `-x` solicita a ativação da autenticação simples. `(objectClass=*)` declara que todos os objetos contidos no diretório devem ser lidos. Esta opção de comando pode ser usada após a criação de uma nova árvore de diretório para verificar se todas as entradas foram registradas corretamente e se o servidor responde como desejado. Mais informações sobre o uso de `ldapsearch` podem ser encontradas na página de manual correspondente (ldapsearch(1)).

45.4.4 Apagando dados de um diretório LDAP

Apague entradas indesejadas com `ldapdelete`. A sintaxe é similar àquela dos comandos descritos acima. Para apagar, por exemplo, a entrada completa para `Tux Linux`, emita o seguinte comando:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

45.5 O cliente LDAP do YaST

O YaST inclui um módulo para configurar o gerenciamento de usuário baseado em LDAP. Se você não habilitou este recurso durante a instalação, inicie o módulo selecionando *Serviços de Rede → Cliente LDAP*. O YaST habilita automaticamente quaisquer alterações relacionadas a PAM e NSS conforme exigido por LDAP (descrito abaixo) e instala os arquivos necessários.

45.5.1 Procedimento padrão

Conhecimento básico sobre os processos agindo no segundo plano de uma máquina cliente ajudam você a compreender como o módulo do cliente LDAP do YaST funciona. Se o LDAP for ativado para autenticação de rede ou o módulo YaST for chamado, os pacotes `pam_ldap` e `nss_ldap` serão instalados e os dois arquivos de configuração correspondentes serão adaptados. `pam_ldap` é o módulo PAM responsável pela negociação entre processos de login e o diretório LDAP como a fonte de dados de autenticação. O módulo dedicado `pam_ldap.so` é instalado e a configuração PAM, adaptada (consulte Exemplo 45.11, “pam_unix2.conf adaptado para LDAP” (p 701)).

Exemplo 45.11 *pam_unix2.conf adaptado para LDAP*

```
auth:       use_ldap
account:    use_ldap
password:   use_ldap
session:    none
```

Ao configurar manualmente serviços adicionais para usar o LDAP, inclua o módulo LDAP do PAM no arquivo de configuração PAM correspondente ao serviço em `/etc/pam.d`. Arquivos de configuração já adaptados a serviços individuais podem ser encontrados em `/usr/share/doc/packages/pam_ldap/pam.d/`. Copie os arquivos apropriados para `/etc/pam.d`.

A resolução de nome `glibc` através do mecanismo `nsswitch` é adaptado ao uso do LDAP com `nss_ldap`. Um arquivo `nsswitch.conf` novo, adaptado é criado em `/etc/` com a instalação deste pacote. Mais informações sobre o funcionamento de `nsswitch.conf` podem ser encontradas em Seção 38.5.1, “Arquivos de configuração” (p 616). As linhas a seguir devem estar presentes em `nsswitch.conf` para a administração do usuário e autenticação com LDAP. Consulte Exemplo 45.12, “Adaptações em nsswitch.conf” (p 701).

Exemplo 45.12 *Adaptações em nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Estas linhas ordenam a biblioteca de resolução de `glibc` primeiro para avaliar os arquivos correspondentes em `/etc` e adicionalmente acessar o servidor LDAP como fontes para dados de usuário e autenticação. Teste este mecanismo, por exemplo, lendo o conteúdo do banco de dados de usuário com o comando `getent passwd`. O conjunto retornado deve conter uma pesquisa dos usuários locais do seu sistema e todos os usuários armazenados no servidor LDAP.

Para evitar que usuários regulares gerenciados através de LDAP efetuem login no servidor com `ssh` ou `login`, os arquivos `/etc/passwd` e `/etc/group` cada precisam incluir uma linha adicional. Esta é a linha `+:::::::/sbin/nologin` em `/etc/passwd` e `+:::` em `/etc/group`.

45.5.2 Configuração do cliente LDAP

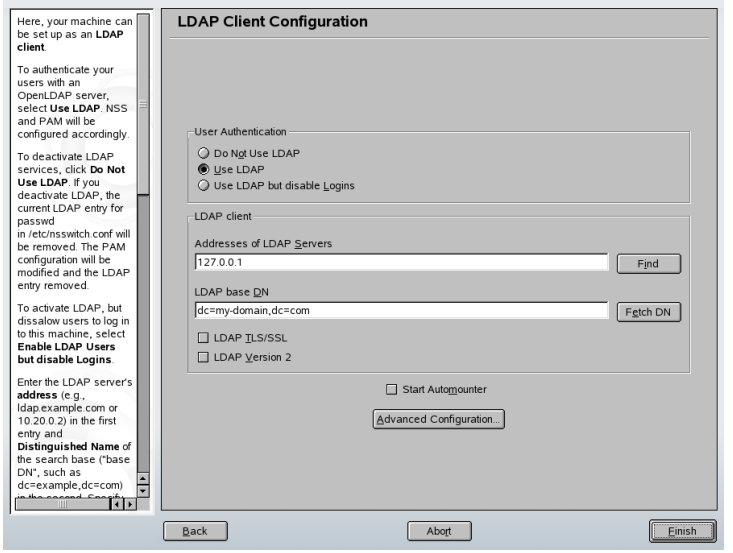
Após os ajustes iniciais de `nss_ldap`, `pam_ldap`, `/etc/passwd` e `/etc/group` terem sido tratados pelo YaST, você pode simplesmente conectar o cliente ao servidor e deixar que o YaST faça o gerenciamento de usuários via LDAP. A configuração básica é descrita em “Configuração Básica” (p 702).

Use o cliente LDAP do YaST para configurar mais os módulos de configuração de usuário e grupo do YaST. Isso inclui manipular as configurações padrão para novos usuários e grupos e o número e a natureza dos atributos atribuídos a um usuário ou grupo. O gerenciamento de usuários LDAP permite atribuir mais atributos e diferentes a usuários e grupos do que as soluções de gerenciamento de grupos ou usuários tradicionais. Isso está descrito em “Configurando os módulos de administração de usuários e grupos do YaST” (p 705).

Configuração Básica

A caixa de diálogo de configuração básica do cliente LDAP (Figura 45.2, “YaST: Configuração do cliente LDAP” (p 703)) abre durante a instalação se você escolher o gerenciamento de usuários LDAP ou quando selecionar *Serviços de Rede → Cliente LDAP* no Centro de Controle do YaST no sistema instalado.

Figura 45.2 *YaST: Configuração do cliente LDAP*


Here, your machine can be set up as an LDAP client.
To authenticate your users with an OpenLDAP server, select Use LDAP. NSS and PAM will be configured accordingly.
To deactivate LDAP services, click Do Not Use LDAP. If you deactivate LDAP, the current LDAP entry for passwd in /etc/nsswitch.conf will be removed. The PAM configuration will be modified and the LDAP entry removed.
To activate LDAP, but dissalow users to log in to this machine, select Enable LDAP Users but disable Logins.
Enter the LDAP server's address (e.g., ldap.example.com or 10.20.0.2) in the first entry and Distinguished Name of the search base ("base DN", such as dc=example,dc=com)
LDAP Client Configuration
User Authentication
Do Not Use LDAP
Use LDAP
Use LDAP but disable Logins
LDAP client
Addresses of LDAP Servers
127.0.0.1
Find
LDAP base DN
dc=my-domain,dc=com
Fetch DN
LDAP TLS/SSL
LDAP Version 2
Start Automounter
Advanced Configuration...
Back
Abort
Finish

Para autenticar usuários da sua máquina em um servidor OpenLDAP e habilitar o gerenciamento de usuários via OpenLDAP, proceda da seguinte maneira:

1. Clique em *Usar LDAP* para habilitar o uso de LDAP. Selecione *Usar LDAP mas Desabilitar Logins* se você deseja usar o LDAP para autenticação, mas não deseja que outros usuários efetuem login neste cliente.

2. Insira o endereço IP do servidor LDAP para uso.

3. Insira a *Base LDAP DN* para selecionar a base de busca no servidor LDAP.

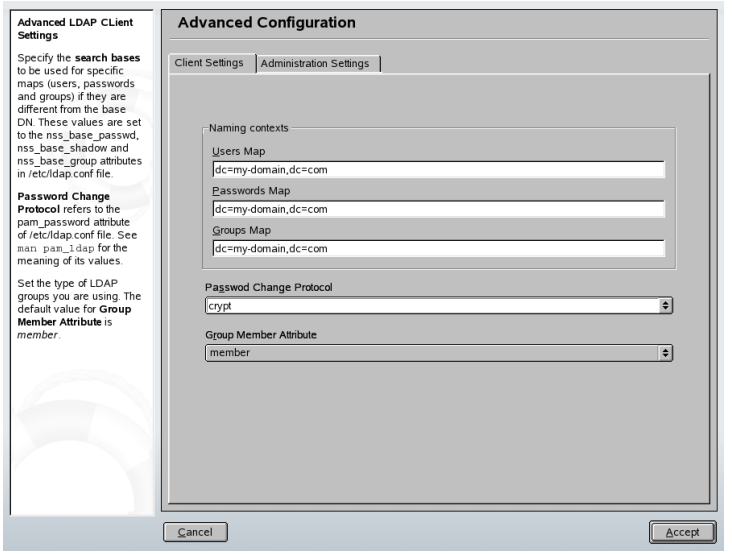
4. Se a comunicação protegida por TLS ou SSL com o servidor for necessária, selecione *LDAP TLS/SSL*.

5. Se o servidor LDAP ainda usar LDAPv2, habilite explicitamente o uso desta versão de protocolo selecionando *LDAP Versão 2*.

6. Selecione *Iniciar Automounter* para montar diretórios remotos no seu cliente como um `/home` gerenciado remotamente.

7. Clique em *Concluir* para aplicar suas configurações.

Figura 45.3 *YaST: Configuração Avançada*


Advanced LDAP CLient Settings
Specify the search bases to be used for specific maps (users, passwords and groups) if they are different from the base DN. These values are set to the nss_base_passwd, nss_base_shadow and nss_base_group attributes in /etc/ldap.conf file.
Password Change Protocol refers to the pam_password attribute of /etc/ldap.conf file. See man pam_ldap for the meaning of its values.
Set the type of LDAP groups you are using. The default value for Group Member Attribute is member.
Advanced Configuration
Client Settings
Administration Settings
Naming contexts
Users Map
dc=my-domain,dc=com
Passwords Map
dc=my-domain,dc=com
Groups Map
dc=my-domain,dc=com
Passwod Change Protocol
crypt
Group Member Attribute
member
Cancel
Accept

Para modificar dados no servidor como administrador, clique em *Configuração Avançada*. A caixa de diálogo seguinte é dividida em duas guias. Consulte Figura 45.3, “YaST: Configuração Avançada” (p 704):

1. Na guia *Configurações do Cliente*, ajuste as seguintes configurações às suas necessidades:

   a. Se a base de busca para usuários, senhas e grupos diferir da base de busca global especificada em *Base LDAP DN*, insira esses contextos de nomeação diferentes em *Mapa do Usuário*, *Mapa da Senha* e *Mapa do Grupo*.

   b. Especifique o protocolo de alteração de senha. O método padrão a ser usado sempre que uma senha é alterada é `crypt`, significando que os hashes de senha gerados por `crypt` são usados. Para obter detalhes sobre esta e outras opções, consulte a página de manual de `pam_ldap`.

   c. Especifique o grupo LDAP a ser usado com *Atributo de Membro de Grupo*. O valor padrão para isso é `membro`.

2. Em *Configurações da Administração*, ajuste as seguintes configurações:

a Defina a base para armazenar os dados do gerenciamento de usuários via *Base de Configuração DN*.

b Insira o valor apropriado para *DN do Administrador*. Este DN deve ser idêntico ao valor `rootdn` especificado em `/etc/openldap/slapd.conf` para habilitar este usuário específico a manipular dados armazenados no servidor LDAP.

c Marque *Criar Objetos de Configuração Padrão* para criar os objetos de configuração básica no servidor para habilitar o gerenciamento de usuários via LDAP.

d Se a máquina do cliente deve agir como um servidor de arquivos para diretórios pessoais na rede, marque *Diretórios Pessoais nesta Máquina*.

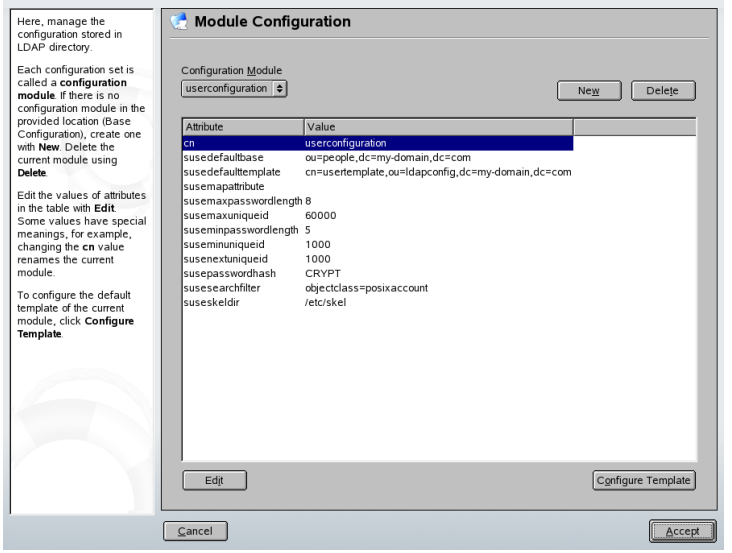
e Clique em *Aceitar* para sair de *Configuração Avançada* e em *Concluir* para aplicar suas configurações.

Use *Definir Configurações de Gerenciamento de Usuários* para editar entradas no servidor LDAP. Acesso aos módulos de configuração no servidor é então concedido de acordo com os ACLs e ACIs armazenados no servidor. Siga os procedimentos apresentados em "Configurando os módulos de administração de usuários e grupos do YaST" (p 705).

Configurando os módulos de administração de usuários e grupos do YaST

Use o cliente LDAP do YaST para adaptar os módulos YaST para administração de grupo e usuários e estendê-los conforme necessário. Defina modelos com valores padrão para os atributos individuais para simplificar o registro de dados. As predefinições criadas aqui são armazenadas como objetos LDAP no diretório LDAP. O registro de dados de usuários ainda é realizado com módulos YaST regulares para o gerenciamento de grupos e usuários. Os dados registrados são armazenados como objetos LDAP no servidor.

Figura 45.4 *YaST: Configuração do módulo*



A caixa de diálogo para configuração do módulo (Figura 45.4, “YaST: Configuração do módulo” (p 706)) permite a criação de novos módulos, a seleção e modificação de módulos de configuração existentes e o design e a modificação de modelos para estes módulos.

Para criar um novo módulo de configuração, proceda da seguinte maneira:

1. Clique em *Novo* e selecione o tipo de módulo a ser criado. Para um módulo de configuração de usuários, selecione `suseuserconfiguration` e para configuração de grupos, selecione `susegroupconfiguration`.

2. Escolha um nome para o novo modelo.

   A visão de conteúdo apresenta uma tabela listando todos os atributos permitidos neste módulo com seus valores atribuídos. Fora dos atributos definidos, a lista também contém todos os outros atributos permitidos pelo esquema atual, mas que não são usados atualmente.

3. Aceite os valores predefinidos ou ajuste os padrões para usar na configuração de usuários e grupos selecionando o respectivo atributo, pressionando *Editar* e

inserindo o novo valor. Renomeie um módulo alterando o atributo `cn` do módulo. Clicar em *Apagar* apaga o módulo atualmente selecionado.

4 Após clicar em *OK*, o novo módulo será adicionado ao menu de seleção.

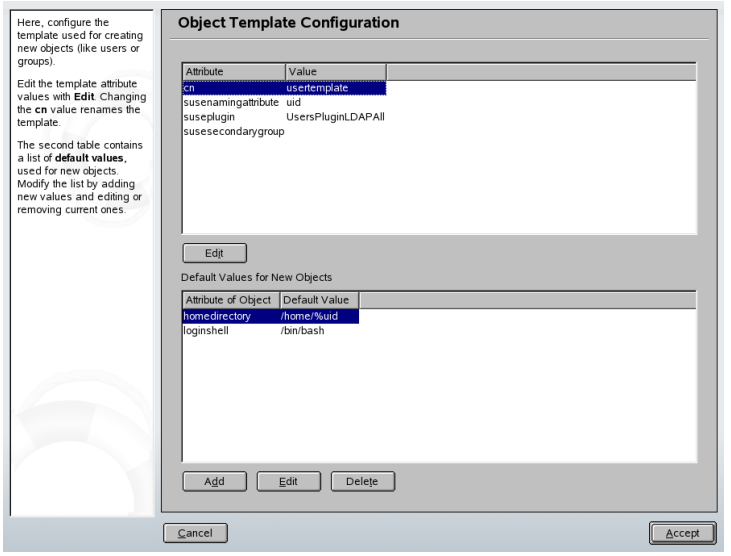
Os módulos YaST para a administração de usuários e grupos embute modelos com valores padrão sensíveis. Para editar um modelo associado a um módulo de configuração, proceda da seguinte maneira:

1 Na caixa de diálogo *Configuração do Módulo*, clique em *Configurar Modelo*.

2 Determine os valores dos atributos gerais atribuídos a este modelo de acordo com suas necessidades ou deixe alguns vazios. Atributos vazios são apagados no servidor LDAP.

3 Modifique, apague ou adicione novos valores padrão para novos objetos (objetos de configuração de grupos ou usuários na árvore LDAP).

Figura 45.5 *YaST: Configuração de um modelo de objeto*



Conecte o modelo ao seu módulo definindo o valor de atributo `susedefaulttemplate` do módulo ao DN do módulo adaptado.

DICA

Os valores padrão para um atributo podem ser criados de outros atributos usando um estilo variável em vez de um valor absoluto. Por exemplo, ao criar um novo usuário, `cn=%sn %givenName` é criado automaticamente dos valores de atributos para `sn` e `givenName`.

Após todos os módulos e modelos terem sido configurados corretamente e estarem prontos para execução, novos grupos e usuários podem ser registrados da maneira usual com o YaST.

45.6 Configurando grupos e usuários LDAP no YaST

O registro atual de dados de grupos e usuários difere apenas um pouco do procedimento quando LDAP não está sendo usado. As seguintes instruções breves estão relacionadas à administração dos usuários. O procedimento para administrar grupos é análogo.

1. Acesse a administração do usuário YaST com *Segurança & Usuários* → *Administração de Usuário*.

2. Use *Definir Filtros* para limitar a exibição de usuários aos usuários LDAP e insira a senha para DN raiz.

3. Clique em *Adicionar* e insira a configuração de um novo usuário. Uma caixa de diálogo com quatro guias é aberta:

   a. Especifique nome de usuário, login e senha na guia *Dados do Usuário*.

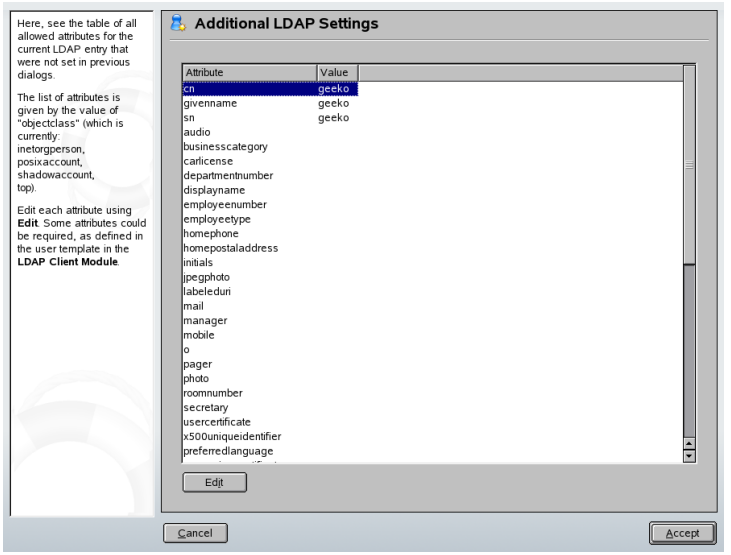
   b. Marque a guia *Detalhes* para a participação de grupo, shell de login e diretório pessoal do novo usuário. Se necessário, altere o padrão para valores que melhor atendem suas necessidades. Os valores padrão e as configurações de senha podem ser definidos com o procedimento descrito em "Configurando os módulos de administração de usuários e grupos do YaST" (p 705).

   c. Modifique ou aceite as *Configurações de Senha* padrão.

d Vá para a guia *Plug-Ins*, selecione o plug-in do LDAP e clique em *Iniciar* para configurar atributos LDAP adicionais atribuídos ao novo usuário (consulte Figura 45.6, “YaST: Configurações LDAP adicionais” (p 709)).

4 Clique em *Aceitar* para aplicar suas configurações e saia da configuração do usuário.

Figura 45.6 *YaST: Configurações LDAP adicionais*



A forma de entrada inicial da administração do usuário oferece *Opções do LDAP*. Isso fornece a possibilidade de aplicar filtros de busca do LDAP para o conjunto de usuários disponíveis ou ir para o módulo para a configuração de grupos e usuários LDAP selecionando *Configuração de Grupos e Usuários LDAP*.

45.7 Para obter mais informações

Assuntos mais complexos, como a configuração de SASL ou o estabelecimento de um servidor LDAP de replicação que distribui a carga de trabalho entre vários escravos, intencionalmente não foi incluída neste capítulo. Informações detalhadas sobre ambos

os assuntos podem ser encontradas no *Guia do Administrador do OpenLDAP 2.2* (referências a seguir).

O website do projeto OpenLDAP oferece documentação exaustiva para usuários LDAP iniciantes e avançados:

OpenLDAP Faq-O-Matic
: Uma coleção abrangente de perguntas e respostas referentes à instalação, configuração e ao uso do OpenLDAP. Encontre-o em `http://www.openldap.org/faq/data/cache/1.html`.

Guia Rápido de Início
: Instruções breves etapa por etapa para instalar o seu primeiro servidor LDAP. Encontre-o em `http://www.openldap.org/doc/admin22/quickstart.html` ou em um sistema instalado em `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`.

Guia do Administrador do OpenLDAP 2.2
: Uma introdução detalhada para todos os aspectos importantes da configuração do LDAP, incluindo criptografia e controles de acesso. Consulte `http://www.openldap.org/doc/admin22/` ou, em um sistema instalado, `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

Compreendendo o LDAP
: Uma introdução geral detalhada para os princípios básicos do LDAP: `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`.

Literatura impressa sobre o LDAP:

- *LDAP System Administration* por Gerald Carter (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* por Howes, Smith e Good (ISBN 0-672-32316-8)

O material de referência mais importante sobre o LDAP são os RFCs (request for comments) correspondentes, 2251 a 2256.

46 O servidor Web do Apache

Com uma cota de mais de 60%, Apache é o servidor Web mais usado mundialmente de acordo com http://www.netcraft.com. Nos aplicativos Web, o Apache é geralmente usado em Linux, com o banco de dados MySQL e as linguagens de programação PHP e Perl. Esta combinação é comumente conhecida como LAMP.

Este capítulo introduz o software do servidor de aplicativos e Web do Apache na versão 2.x. A instalação e configuração do Apache são explicadas aqui, junto com o uso de alguns dos módulos disponíveis.

46.1 Prefácio e terminologia

Esta seção fornece definições de termos usados com freqüência, tanto relacionados à Web como específicos do Apache.

IMPORTANTE: Terminologia

Neste documento, o termo *Apache* refere-se ao Apache na versão 2.x. Para a documentação do Apache 1.x, consulte o site do Apache na Web.

46.1.1 Servidor Web

Um servidor Web fornece páginas da Web solicitadas por um cliente. O cliente pode ser um navegador da Web, como o Konqueror, ou qualquer outro dispositivo que possa conectar-se à World Wide Web. Essas páginas podem ser armazenadas como um todo

em disco (páginas estáticas) ou geradas em resposta a uma consulta (páginas dinâmicas) de um entidade externa, como um banco de dados ou um serviço Web.

46.1.2 HTTP

A comunicação entre o cliente e o servidor Web ocorre com o hypertext transfer protocol (HTTP). A versão atual, HTTP 1.1, é documentada no RFC 2068 e na atualização RFC 2616. Esses RFCs estão disponíveis em `http://www.w3.org`.

46.1.3 URLs

URL corresponde a universal resource locator. Os clientes usam URLs, como `http://www.example.com/index.html`, para solicitar páginas do servidor. Um URL contém:

Protocolo
Protocolos usados com freqüência:

http://
O protocolo HTTP

https://

Versão segura e criptografada do HTTP

ftp://

File transfer protocol para fazer download e upload

Domínio

Neste exemplo, o domínio é `www.example.com`. O domínio é o nome que corresponde a um endereço IP. Dessa forma, `www.example.com` mapeia exclusivamente para um endereço IP como 123.456.789.1. Por sua vez, o número identifica exclusivamente o computador executando um servidor Web. O mapeamento de um nome de domínio para um endereço IP é comumente conhecido como uma *resolução de nomes*. O domínio pode ser subdividido em várias partes, como a seguir: `www`, `example` e `com`. A última parte do nome de domínio é o domínio superior (TLD). Neste exemplo, `com` é o TLD. TLD representa o nível

superior do processo de resolução de nomes. TLDs podem ser genéricos (gTLDs, como `com`, `org` e `net`) ou específicos do país (ccTLDs, como `de` para Alemanha). Todas as partes de um domínio juntas são conhecidas como nome de domínio completo (FQDN).

Recurso
Neste exemplo, o recurso é `index.html`. Esta parte especifica o caminho completo do recurso. O recurso pode ser um arquivo, como neste exemplo. No entanto, ele também pode ser um script CGI, uma página JavaServer ou algum outro recurso.

O mecanismo da Internet responsável, como o DNS (domain name system) encaminha a consulta ao domínio `www.example.com` para um ou vários computadores que contêm o recurso. O Apache fornece o recurso real, neste exemplo, a página `index.html`, ao cliente. Neste caso, o arquivo está localizado no diretório de nível superior. No entanto, recursos também podem estar localizados em subdiretórios, como em `http://www.example.com/linux/novell/suse`.

46.1.4 Diretiva

Para configurar o Apache, o termo *diretiva* é geralmente usado como sinônimo para "opção de configuração." Diretiva é o termo técnico relativo ao software do servidor Web do Apache.

46.2 Instalação

O Apache no SUSE Linux é executado "fora da caixa" com uma configuração padrão e predefinida. Se seguir as instruções neste capítulo, o servidor Web do Apache estará funcionando em pouco tempo. Você deve ser `root` para instalar e configurar o Apache.

46.2.1 Instalando o Apache com o YaST

O pacote apache2 para SUSE Linux é um pouco diferente em seu sistema de arquivos e layout de aplicativo em relação ao pacote de software padrão disponível no site do Apache (`http://httpd.apache.org`). A seção a seguir descreve detalhadamente a instalação desse pacote e indica as variações quando aplicáveis.

Para instalar um servidor Web simples, faça o seguinte:

Procedimento 46.1 *Instalação rápida*

1. Inicie o YaST no modo de interface padrão ou de linha de comando.
2. Selecione *Serviços de Rede → Servidor HTTP*.
3. Clique em *Continuar* para confirmar a instalação dos pacotes `apache2` e `apache2-prefork`.
4. Uma vez concluída a instalação, o *Assistente de Configuração do Apache* é exibido, e você pode iniciar a configuração do servidor Web.

A desvantagem de seguir o procedimento acima é que não há suporte a banco de dados e PHP. Para instalar um servidor Web com esse suporte, faça o seguinte:

Procedimento 46.2 *Instalação de servidor Web simples*

1. Inicie o YaST no modo de interface padrão ou de linha de comando.
2. Selecione *Software → Instalar e Remover Software*.
3. Selecione *Seleções* em *Filtro* e marque *Servidor da Web Simples com Apache2*.
4. Pressione *OK*.
5. Confirme a instalação dos pacotes dependentes para concluir o processo de instalação do Apache2 para SUSE Linux.

Para usuários avançados, o SUSE Linux oferece uma seleção de pacotes personalizados. Para executar uma instalação personalizada de um servidor Web, faça o seguinte:

Procedimento 46.3 *Instalação do RPM padrão do Apache com o YaST*

1. Inicie o YaST no modo de interface padrão ou de linha de comando. Selecione *Software → Instalar e Remover Software*.
2. Selecione *Pesquisar* em *Filtro* e digite `apache2` no campo *Pesquisar*.
3. Selecione `apache2` para instalação.

4 Use as etapas 2 e 3 para a seleção do módulo. Consulte a Seção 46.5, “Módulos do Apache” (p 741).

5 Após a seleção, pressione *Aceitar*.

6 Em seguida, você deverá escolher uma das dependências para o pacote `apache2-MPM` necessário: `apache2-prefork` ou `apache2-worker`. Consulte a Seção 46.2.2, “Módulos de multiprocessamento” (p 715) para obter uma explicação das diferenças entre os dois. Se você estiver em dúvida, selecione o pacote `apache2-prefork`, que é o padrão para os sistemas operacionais baseados em Unix, e pressione *OK*.

7 Confirme a instalação dos pacotes dependentes para concluir o processo de instalação do Apache2 para SUSE Linux.

NOTA: Iniciando um servidor Web

A instalação do Apache não inicia automaticamente o servidor Web. Consulte a Seção 46.3.3, “Ativando, iniciando e parando o Apache” (p 735) para obter informações sobre como controlar a inicialização e o encerramento do Apache.

46.2.2 Módulos de multiprocessamento

Conforme mencionado em Instalação do RPM padrão do Apache com o YaST (p 714), o SUSE Linux oferece dois módulos de multiprocessamento (MPMs) diferentes para uso com o Apache. Os MPMs são responsáveis pela aceitação e manipulação de solicitações ao servidor Web, representando o centro do software do servidor Web.

MPM prefork

O MPM prefork implementa um servidor Web de pré-bifurcação não encadeado. Ele faz com que o servidor Web comporte-se de maneira semelhante ao Apache versão 1.x no sentido de que ele isola as solicitações e as trata através da pré-bifurcação de um processo-filho separado . Dessa forma, solicitações problemáticas não podem afetar outros, evitando um bloqueio do servidor Web.

Embora o MPM prefork ofereça estabilidade com esta abordagem baseada em processo, ele consome mais recursos do sistema do que o seu equivalente, o MPM worker. O

MPM prefork é considerado o MPM padrão para sistemas operacionais baseados em Unix.

IMPORTANTE: MPMs neste documento

Este documento pressupõe que o Apache é usado com o MPM prefork.

MPM worker

O MPM worker oferece um servidor Web multiencadeado. Encadeamento é uma forma "mais simples" de um processo. A vantagem de um encadeamento em relação a um processo é o consumo de recursos mais baixo. Em vez de somente pré-bifurcar processos-filhos, o MPM worker serve solicitações usando encadeamentos com processos do servidor. Os processos-filhos pré-bifurcados são multiencadeados.

Essa abordagem faz com que o Apache tenha um melhor desempenho, consumindo menos recursos do sistema do que o MPM prefork. Uma grande desvantagem é a estabilidade do MPM worker: se um encadeamento se torna corrupto, todos os encadeamentos de um processo podem ser afetados. No pior dos casos, isso poderá resultar em uma falha do servidor. Talvez ocorram erros do servidor interno devido a encadeamentos que não podem se comunicar com recursos do sistema, sobretudo ao usar o CGI (descrito na "Interface de Gateway Comum: `mod_cgi` " (p 743)) com o Apache em uma carga pesada.

Outro argumento contra o uso do MPM worker com o Apache é que nem todos os módulos Apache disponíveis (consulte a Seção 46.5, "Módulos do Apache" (p 741)) são seguros para o processo e, portanto, não podem ser usados em conjunto com o MPM worker.

ATENÇÃO: PHP como um módulo do Apache (`mod_php`)

Nem todos os módulos PHP disponíveis são seguros para o processo. O uso do MPM worker com `mod_php` é bastante desestimulado.

46.2.3 Sistema de arquivos padrão e layout de aplicativos

O SUSE Linux coloca os arquivos do pacote Apache em locais padrão. Os locais dos arquivos mais importantes estão listados aqui.

Binários

A maioria dos arquivos executáveis do SUSE Linux Apache contém um `2` anexado a eles. Isso simplifica a diferenciação de arquivos binários de uma instalação do Apache 1.x paralela ao Apache 2.x.

`/usr/sbin/httpd2`
Link simbólico que aponta para o módulo de multiprocessamento escolhido conforme descrição contida em Seção 46.2.2, “Módulos de multiprocessamento” (p 715). O padrão é `httpd2-prefork`. O link simbólico é mantido pelo script de inicialização de acordo com a configuração do sistema do MPM.

`/usr/sbin/httpd2-prefork`
O Apache2 executável propriamente dito.

`/usr/sbin/apache2ctl`
Script de controle para iniciar e parar o servidor Web, fornecido pelo projeto HTTPD do Apache. Consulte Seção 46.3.3, “Ativando, iniciando e parando o Apache” (p 735) para obter mais informações ou execute `/usr/sbin/apache2ctl help`.

`/etc/init.d/apache2`
Inicia e pára o script proporcionando total integração na instalação do SUSE Linux e iniciando o Apache no momento da inicialização. Ele verifica se há uma configuração válida antes de iniciar e parar o servidor, e substitui o local da configuração. Permite a fácil inclusão de arquivos de configuração adicionais, do carregamento de módulos, ou mesmo do início de uma instância separada do servidor sem modificação do script.

`/usr/sbin/rcapache2`
Um link simbólico prático para `/etc/init.d/apache2`, pois `/etc/init.d/` não faz parte do caminho por padrão. Basta usar `rcapache2 start` para iniciar o Apache.

/usr/sbin/htpasswd2
Utilitário para gerar senhas criptografadas para a autenticação baseada em `.htaccess`. Consulte a página do manual `htpasswd2(1)` para obter detalhes sobre o uso da ferramenta.

Arquivos de configuração

A maioria dos arquivos de configuração fica situada em `/etc/apache2`. Para obter informações sobre como fazer mudanças nas configurações, consulte Seção 46.3, “Configuração” (p 720).

/etc/apache2/httpd.conf
Arquivo de configuração de nível superior. Se possível, evite fazer mudanças nesse arquivo. Ele inclui, principalmente, outros arquivos de configuração e declara configurações globais.

/etc/apache2/*.conf
Alguns módulos externos do Apache colocam seus arquivos de configuração no diretório `/etc/apache2/`, normalmente com o próprio nome do módulo como prefixo (`mod_*.conf`).

/etc/apache2/conf.d/*
Diretório que abriga diversos outros arquivos de configuração que vêm em determinados pacotes. Para obter um exemplo, consulte “Servindo o PHP: `mod_php4`, `mod_php5` ” (p 750).

/etc/apache2/vhosts.d/*
Diretório que abriga os arquivos de configuração opcionais dos hosts virtuais. Consulte Seção 46.4, “Hosts virtuais” (p 737) para obter detalhes.

/etc/sysconfig/apache2
Arquivo de configuração do SUSE Linux associado ao Apache2. Ele contém todos os parâmetros de configuração relevantes para o controle do servidor Web do Apache. `/etc/sysconfig/apache2` é usado pelo YaST para configurar o Apache conforme descrição contida em Seção 46.3.1, “Configurando o Apache com o YaST” (p 721). Ele também pode ser editado manualmente conforme descrição em Seção 46.3.2, “Configurando o Apache manualmente” (p 728).

Arquivos de registro

Por padrão, o Apache fornece diversas informações sobre seu status de tempo de execução nos seguintes arquivos:

`/var/log/apache2/error_log`
O Apache registra, nesse arquivo, avisos de inicialização e encerramento, e também todos os erros de tempo de execução.

`/var/log/apache2/access_log`
Todas as solicitações feitas ao servidor Web são registradas nesse arquivo. O formato padrão das entradas é o formato combinado, que mostra informações sobre o host e o agente do usuário emissor da solicitação e o URI de referência.

Root do documento

O diretório físico `/srv/www/htdocs` é o local padrão de onde o Apache dá suporte a páginas da Web. Ele atua como "diretório raiz" para as solicitações de clientes. Para publicar página da Web com o Apache, armazene os arquivos de forma hierárquica dentro do ou sob o diretório

Um URL como http://www.example.com/index.html se refere a `/srv/www/htdocs/index.html` na configuração padrão do Apache no SUSE Linux para um domínio chamado example.com.

46.2.4 Construção manual de módulos

O Apache é feito com uma abordagem modular, ou seja, os módulos fornecem os recursos do próprio software do servidor Web. Conseqüentemente, o Apache pode ser ampliado por usuários avançados através da gravação de módulos personalizados. Consulte as páginas do manual a seguir para obter informações mais detalhadas.

apache2-devel

Para desenvolver módulos para o Apache ou compilar módulos de terceiros, é necessário o pacote `apache2-devel`, além das ferramentas de desenvolvimento correspondentes. O `apache2-devel` também contém as ferramentas `apxs2`, que são necessárias para a compilação de módulos adicionais para o Apache.

apxs2

Os binários do `apxs2` ficam localizados em `/usr/sbin`:

- `/usr/sbin/apxs2`—apropriado para a construção de um módulo de extensão que funciona com qualquer MPM. A instalação fica localizada em `/usr/lib/apache2`.
- `/usr/sbin/apxs2-prefork`—apropriado para os módulos MPM pré-bifurcação. A instalação fica localizada em `/usr/lib/apache2-prefork`.
- `/usr/sbin/apxs2-worker`—apropriado para os módulos MPM pré-bifurcação.

O `apxs2` instala os módulos de tal modo que possam ser usados em todos os MPMs. Os outros dois programas instalam os módulos para que possam ser usados somente nos respectivos MPMs. O `apxs2` instala os módulos em `/usr/lib/apache2` e o `apxs2-prefork` instala os módulos em `/usr/lib/apache2-prefork`.

O `apxs2` permite a compilação e instalação de módulos do código-fonte (inclusive as mudanças necessárias nos arquivos de configuração), que cria *objetos compartilhados dinâmicos* (DSOs) que podem ser carregados no Apache durante a execução. Para instalar um módulo do código-fonte, use os comandos `cd /path/to/module/source; apxs2 -c -i mod_foo.c`. Outras opções do `apxs2` são descritas na página do manual `apxs2(1)`. Em seguida, os módulos devem ser ativados em `/etc/sysconfig/apache2` com a entrada `APACHE_MODULES`, conforme descrição contida em Seção 46.3.2, “Configurando o Apache manualmente” (p 728).

46.3 Configuração

O Apache no SUSE Linux pode ser configurado de duas maneiras diferentes: com o YaST ou manualmente. A configuração manual oferece um nível maior de detalhes, mas não tem a conveniência da interface gráfica de usuário do YaST.

IMPORTANTE: Mudanças de configuração

As mudanças a alguns valores de configuração do Apache somente são efetuadas depois que o Apache é reiniciado. Isso ocorre automaticamente ao concluir a

configuração usando o YaST com a opção *Habilitado* selecionada para o *Serviço HTTP*. A reiniciação manual está descrita na Seção 46.3.3, “Ativando, iniciando e parando o Apache” (p 735). A maioria das mudanças de configuração somente requerem um recarregamento com o `rcapache2 reload`.

46.3.1 Configurando o Apache com o YaST

Com o YaST, você pode transformar um host da rede em um servidor Web. Para configurar esse servidor, inicie o YaST e selecione *Serviços de Rede* → *Servidor HTTP*. Quando o módulo é iniciado pela primeira vez, o Assistente de Servidor HTTP é iniciado, solicitando que você tome algumas decisões básicas em relação à administração do servidor.

Assistente de Servidor HTTP

O Assistente de Servidor HTTP consiste em cinco etapas ou caixas de diálogo. Na última etapa da caixa de diálogo, você tem a oportunidade de entrar no modo de configuração técnica para realizar configurações ainda mais específicas.

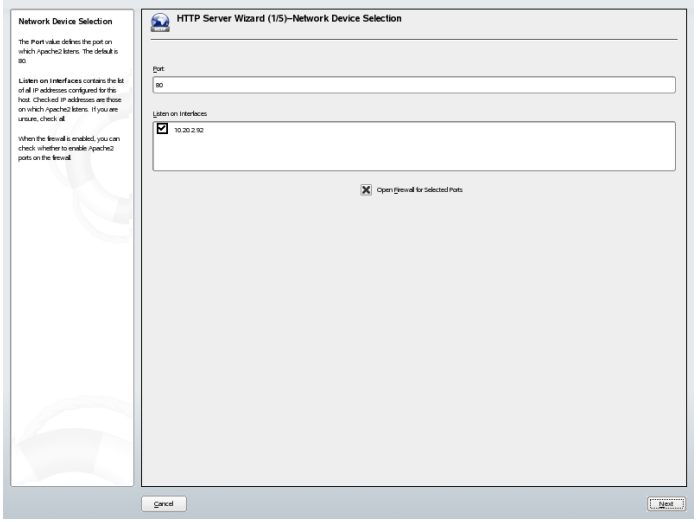
Seleção de dispositivos de rede

Especifique aqui as interfaces e portas de rede usadas pelo Apache para escutar as solicitações recebidas. Você pode selecionar qualquer combinação de interfaces de rede existentes e seus respectivos endereços IP. As portas de todas as três faixas (portas conhecidas, portas registradas e portas dinâmicas ou privadas), que não forem reservadas por outros serviços, poderão ser usadas.

A configuração padrão consiste em escutar em todas as interfaces de rede (endereços IP) na porta 80. Quando o firewall é habilitado, você pode verificar se as portas Apache devem ser habilitadas nele.

Marque *Abrir Firewall nas Portas Selecionadas* para abrir as portas no firewall em que o servidor Web escuta. É necessário tornar um servidor Web disponível na rede, que pode ser uma LAN, uma WAN ou a Internet. Manter a porta de `Escuta` fechada é útil em situações de teste em que não é necessário nenhum acesso externo ao servidor Web. Se você estiver satisfeito com as configurações padrão ou se tiver feito mudanças, clique em *Próximo* para continuar a configuração.

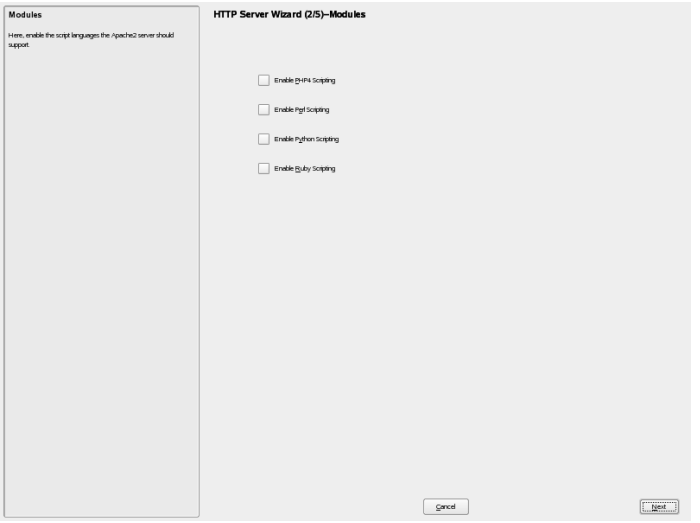
Figura 46.1 *Assistente de Servidor HTTP: Seleção de dispositivos de rede*


Network Device Selection
The Port value defines the port on which Apache2 listens. The default is 80.
Listen on Interfaces contains the list of all IP addresses configured for the host. Checked IP addresses are those on which Apache2 listens. If you are unsure, check all.
When the firewall is enabled, you can check whether to enable Apache2 ports on the firewall.
HTTP Server Wizard (1/5)–Network Device Selection
Port:
80
Listen on Interfaces
10.20.2.92
Open Firewall for Selected Ports
Cancel
Next

Módulos

O pacote Apache para SUSE Linux contém uma grande variedade de módulos Apache. Os módulos estendem a funcionalidade do Apache e estão disponíveis para diversas tarefas. A opção de configuração *Módulos* permite carregar e descarregar vários módulos Apache quando o servidor é iniciado. Para obter uma explicação mais detalhada dos módulos, consulte a Seção 46.5, “Módulos do Apache” (p 741). Clique em *Próximo* para continuar.

Figura 46.2 *Assistente de Servidor HTTP: Módulos*

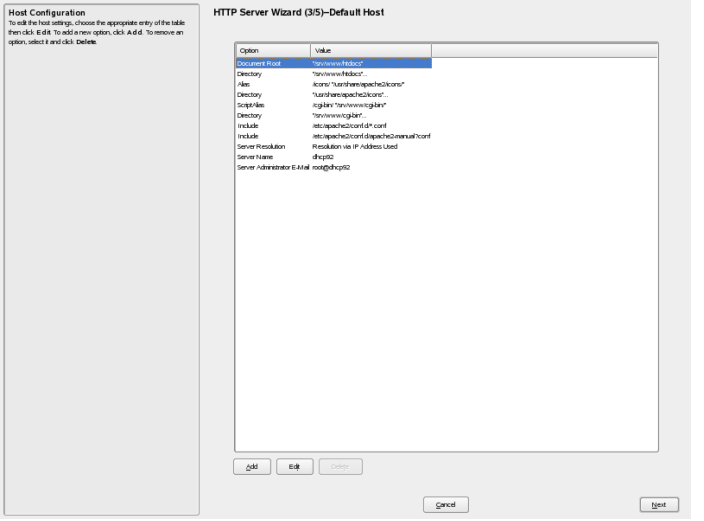


Host padrão

Esta opção pertence ao servidor Web padrão. Como explicado na Seção 46.4, "Hosts virtuais" (p 737), o Apache pode atender a vários domínios de uma única máquina física. O primeiro domínio declarado (ou `VirtualHost`) no arquivo de configuração é normalmente conhecido como *Host Padrão*. Para editar as configurações do host, escolha a entrada adequada na tabela e clique em *Editar*. Para adicionar um novo host, clique em *Adicionar*. Para apagar um host, selecione-o e clique em *Excluir*.

Nessa etapa, você pode decidir adicionar um valor e uma opção SSL (secure sockets layer) para as configurações do host. Você pode ler mais sobre isso em "Adicionando o suporte SSL" (p 728).

Figura 46.3 *Assistente de Servidor HTTP: Host padrão*



Esta é a lista das configurações padrão do servidor:

Root do documento
Como descrito em “Root do documento” (p 719), `/srv/www/htdocs` é o local padrão de onde o Apache dá suporte a páginas da Web.

Diretório
`/srv/www/htdocs` é o local das páginas da Web.

Álias
Com a ajuda das diretivas `Alias`, os URLs podem ser mapeados para locais físicos do sistema de arquivos. Isso significa que determinado caminho mesmo *fora* de `Document Root` no sistema de arquivos pode ser acessado por meio de um URL que serve de álias para esse caminho.

O diretório padrão `Alias /icons` do SUSE Linux aponta para `/usr/share/apache2/icons` para os ícones do Apache exibidos na tela de índice do diretório.

Diretório
`/usr/shareapache2/icons` é o local do diretório `Alias`.

Álias de script
Semelhante à diretiva `Alias`, a diretiva `ScriptAlias` mapeia um URL para o local do sistema de arquivos. A diferença é que `ScriptAlias` designa o diretório de destino como um local CGI, significando que os scripts CGI devem ser executados nesse local.

Diretório
`/srv/www/cgi-bin` é o local do diretório `ScriptAlias`.

Inclusão
`/etc/apache2/conf.d/*.conf` é o diretório que contém os arquivos de configuração que acompanham determinados pacotes. `/etc/apache2/conf.d/apache2-manual?conf` é o diretório que contém todos os arquivos de configuração `apache2-manual`.

Resolução do servidor
Esta opção refere-se à Seção 46.4, “Hosts virtuais” (p 737).

Determinar Servidor que Solicita por Cabeçalhos HTTP permite uma resposta do `VirtualHost` em uma solicitação a seu servidor de nomes (consulte Seção 46.4.1, “Hosts virtuais baseados em nome” (p 737)).

Determinar Servidor que Solicita por Endereço IP faz com que o Apache selecione o host solicitado, de acordo com as informações de cabeçalho HTTP enviadas pelo cliente. Consulte a Seção 46.4.2, “Hosts virtuais baseados em IP” (p 739) para obter mais detalhes sobre hosts virtuais baseados em IP.

Nome do Servidor
Especifica o URL padrão usado por clientes para entrar em contato com o servidor Web. Use um FQDN (consulte Domínio (p 712)) para acessar o servidor Web em `http://`*`FQDN`* ou seu endereço IP.

E-Mail do Administrador do Servidor
Forneça o endereço de e-mail do administrador do servidor Web para *E-Mail do Administrador do Servidor*.

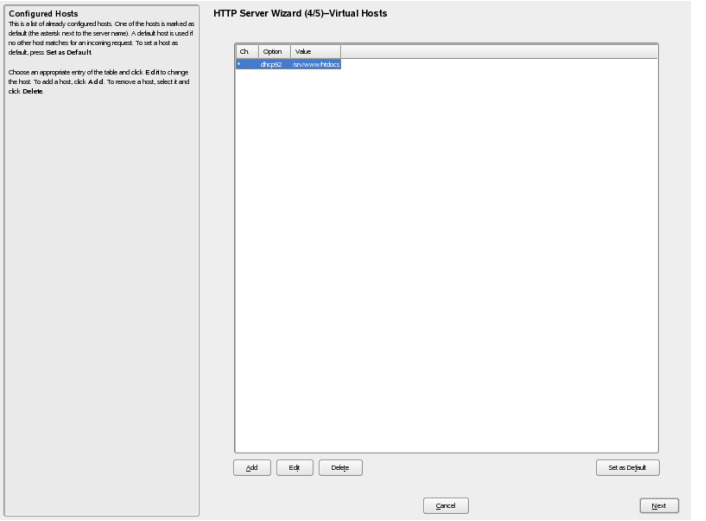
Após concluir a etapa do *Host Padrão*, clique em *Próximo* para continuar na caixa de diálogo de configuração.

Hosts virtuais

Nesta etapa, o assistente exibe uma lista dos hosts virtuais já configurados (consulte aSeção 46.4, “Hosts virtuais” (p 737)). Um dos hosts está marcado como padrão (com um asterisco ao lado do nome do servidor). Para definir um host padrão, selecione o servidor e clique em *Definir como Padrão*.

Para adicionar um host, clique em *Adicionar* e uma caixa de diálogo será exibida para a inserção de informações básicas sobre o host. *Identificação de Servidor* contém o nome do servidor, a raiz do conteúdo do servidor e o e-mail do administrador. O texto de ajuda no quadro esquerdo da janela explica cada um desses itens em detalhes. *Resolução do Servidor* é usado para determinar como um host é identificado. Você pode especificar se deve determinar um servidor de solicitações com base em cabeçalhos HTTP ou por endereço IP do servidor, selecionando a respectiva opção. A outra possibilidade consiste em determinar o host virtual pelo endereço IP usado pelo cliente durante a conexão com o servidor. Você também pode habilitar o suporte SSL marcando essa opção. Também é possível especificar o caminho do arquivo de certificados. Quando você clica em *Pesquisar*, o diretório padrão `/etc/apache2/ssl.crt` é exibido. Após digitar todas as informações, clique em *Próximo* a fim de ir para a etapa final da configuração.

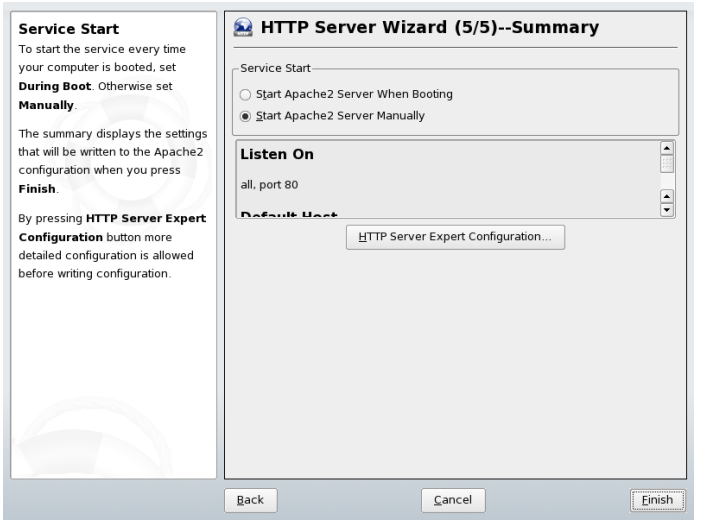
Figura 46.4 *Assistente de Servidor HTTP: Hosts virtuais*



Resumo

Esta é a etapa final do assistente. Determine como e quando o servidor Apache deve ser iniciado: durante a inicialização ou manualmente. A porta selecionada anteriormente também é exibida com nos hosts padrão e virtual. Se você estiver satisfeito com as configurações, clique em *Concluir* para concluir a configuração.

Figura 46.5 *Assistente de Servidor HTTP: Resumo*


Service Start
To start the service every time your computer is booted, set During Boot. Otherwise set Manually.
The summary displays the settings that will be written to the Apache2 configuration when you press Finish.
By pressing HTTP Server Expert Configuration button more detailed configuration is allowed before writing configuration.
HTTP Server Wizard (5/5)--Summary
Service Start
Start Apache2 Server When Booting
Start Apache2 Server Manually
Listen On
all, port 80
HTTP Server Expert Configuration...
Back
Cancel
Finish

Configuração Técnica do Servidor HTTP

O módulo Servidor HTTP também permite que você faça mais ajustes à configuração. Clique em *Configuração Especialista de Servidor HTTP* para ver mais opções de configuração. As seguintes mudanças podem ser feitas:

Escutar em

Quando você seleciona a configuração *Escutar em* e clica em *Editar*, é aberta uma nova janela na qual é possível adicionar, apagar ou editar entradas.

Módulos

Selecionando as configurações *Módulos* e clicando em *Editar*, você pode mudar o status dos módulos Apache2 clicando em *Alternar Status*. Clique em *Adicionar Módulo* para adicionar um novo módulo.

Host Padrão
Para editar as configurações do host, selecione *Host Padrão* e clique em *Editar*. Você também pode adicionar, editar ou apagar opções.

Hosts
Para adicionar, apagar, editar ou selecionar um host como padrão, selecione *Hosts* e clique em *Editar*.

Em todas as caixas de diálogo anteriores, você pode clicar em *Arquivos de Registro* para ver o os registros de erro e de acesso. Clique em *OK* para concluir a configuração e retornar ao Centro de controle do YaST.

Adicionando o suporte SSL

Para adicionar uma opção SSL ao host, clique em *Adicionar* na etapa três (host padrão) do Assistente de Servidor HTTP. Se o servidor já tiver sido configurado e você não tiver mais acesso ao assistente, configure uma opção SSL selecionando *Hosts padrão* na caixa de diálogo Configuração de Servidor HTTP ou clicando em *Editar* e *Adicionar*. Nos dois casos, uma janela pop-up é exibida para que você vá até uma opção *SSL* e confirme com *OK*. Em seguida, você deve digitar um valor para a opção selecionada. Esse procedimento pode ser tão simples quanto definir o valor como *ativar* ou *desativar*; contudo, pode ser necessário digitar um valor adequado. Se estiver em dúvida, consulte a documentação para obter os parâmetros de valor para a configuração do SSL. Depois que você clica em *OK*, a opção e o valor são exibidos na lista de configuração de host. Clique em *Próximo* a fim de ir para a próxima etapa da caixa de diálogo de configuração.

Se *SSL* for exibido na lista de configuração de host, clique em *Editar* para abrir a caixa de diálogo de configuração de SSL. Se ela não for exibida, clique em *Adicionar*, selecione *SSL* e *OK* para que a caixa de diálogo seja aberta automaticamente. Adicione, apague ou edite as opções de SSL. Clique em *OK* para retornar ao Assistente de Servidor HTTP.

46.3.2 Configurando o Apache manualmente

A configuração manual do Apache requer a edição dos arquivos de configuração de texto simples como o usuário `Root`.

IMPORTANTE: Sem o módulo SuSEconfig do Apache2

O módulo SuSEconfig do Apache2 foi removido do SUSE Linux. Ele deixou de ser necessário para a execução do `SuSEconfig` após a mudança de `/etc/sysconfig/apache2`.

/etc/sysconfig/apache2

O `/etc/sysconfig/apache2` controla algumas configurações globais do Apache, como módulos para carregar, arquivos de configuração adicionais para incluir, sinalizadores com os quais o servidor deve ser iniciado e sinalizadores que devem ser adicionados à linha de comando. Como toda opção de configuração desse arquivo está amplamente documentada, não são citadas aqui. No caso de um servidor Web de finalidade geral, `/etc/sysconfig/apache2` deve bastar para as necessidades de configuração. Se uma configuração específica for necessária, consulte "Diretivas do Apache em /etc/apache2/httpd.conf: Ambiente global " (p 730).

IMPORTANTE: Arquivos criados automaticamente na inicialização do servidor

O `/etc/sysconfig/apache2` cria ou edita os seguintes arquivos automaticamente quando o servidor Web é iniciado ou reiniciado.

- `/etc/apache2/sysconfig.d/loadmodule.conf`—módulos carregados durante a execução
- `/etc/apache2/sysconfig.d/global.conf`—configurações gerais aplicadas ao servidor inteiro
- `/etc/apache2/sysconfig.d/include.conf`—lista de arquivos de configuração inclusos

Não edite esses arquivos manualmente. Em vez disso, edite as configurações correspondentes em `/etc/sysconfig/apache2`.

Para ter acesso a ajustes de configuração detalhados, consulte os arquivos contidos em `/etc/apache2/*`, verificando especificamente mudanças na configuração manual dos hosts virtuais, do ambiente global ou do servidor principal.

Diretivas do Apache em /etc/apache2/httpd.conf: Ambiente global

O SUSE Linux usa o `/etc/apache2/httpd.conf` como o ponto central de referência para outros arquivos de configuração. Edite o arquivo somente para habilitar recursos que não estão disponíveis em `/etc/sysconfig/apache2`. As diretivas contidas na seção *Ambiente Global* de `httpd.conf` afetam o funcionamento geral do Apache.

As seções a seguir descrevem algumas das diretivas que não estão disponíveis em YaST. Diretivas básicas como `Root do Documento` (Root do documento (p 724)) são essenciais e obrigatórias tanto no `Ambiente Global` como em `VirtualHost`.

Os parâmetros e diretivas a seguir são ordenados por afiliação lógica e escopo de configuração. Todos eles devem ser definidos em `/etc/apache2/httpd.conf`.

`LoadModule` *`module_identifier /path/to/module`*

A diretiva `LoadModule` especifica um módulo do Apache a ser carregado durante a execução. *`module_identifier`* é o nome do módulo de acordo com sua documentação. */path/to/module* pode ser um caminho absoluto ou relativo que aponte para o arquivo.

Exemplo 46.1 *LoadModule Diretiva*

```
LoadModule rewrite_module /usr/lib/apache2-prefork/mod_rewrite.so
```

No SUSE Linux, não é necessário usar instruções do `LoadModule` diretamente. Em vez disso, o `APACHE_MODULE` é usado em `/etc/sysconfig/apache2`.

`MaxClients` *`número`*

O número máximo de clientes que o Apache pode processar simultaneamente. O porte do MaxClients precisa ser grande o suficiente para que ele processe o número de solicitações simultâneas que o site espere receber, mas pequeno o suficiente para assegurar que haja memória RAM física suficiente para todos os processos.

Tempo de espera *segundos*

Especifica o período de tempo que o Apache deve aguardar antes de reportar um tempo de espera para uma solicitação.

Diretivas do Apache em /etc/apache2/httpd.conf: Servidor principal

As diretivas da seção `Servidor Principal` se aplicam quando solicitações do cliente não são tratadas pelo `VirtualHost` e, portanto, precisam ser processadas por um servidor padrão ou principal. Além disso, os parâmetros definidos nesse contexto são os padrões de todos os hosts virtuais configurados. Conseqüentemente, todas as diretivas do `Servidor Principal` também podem ser definidas no contexto do `VirtualHost`, substituindo os padrões.

DirectoryIndex *nomes de arquivos*

Define quais arquivos o Apache deve pesquisar para completar um URL desprovido de uma especificação de arquivo. A configuração padrão é `index.html`. Por exemplo, se o cliente solicitar o URL `http://www.example.com/foo/` e o diretório `foo` contiver um arquivo chamado `index.html`, o Apache fornece essa página ao cliente. Para declarar vários arquivos, separe-os com espaços.

Exemplo 46.2 *DirectoryIndex Diretiva*

```
DirectoryIndex index.html index.shtml start.php begin.pl
```

AllowOverride Todos | Nenhum | *opção*

Essa diretiva *somente* pode ser usada no interior de uma declaração `<Diretório></Diretório>`. Consulte Diretório (p 724).

`AllowOverride` especifica quais opções de acesso e exibição um arquivo `.htaccess` (ou outros arquivos especificados por `AccessFileName` conforme descrição em "`AccessFileName` *`nomes de arquivos`*" (p 733)) pode substituir.

Valores possíveis:

Tudo
Todas as opções podem ser substituídas por um arquivo `.htaccess`.

Nenhum
Nenhuma das opções pode ser substituída por um arquivo `.htaccess`.

AuthConfig
Os diretórios podem ser protegidos por senha com a ajuda de um arquivo `.htaccess`.

FileInfo
Permite o uso de diretivas que controlam os tipos de documentos no interior de um arquivo `.htaccess`. Um exemplo típico disso é a configuração de páginas de erro personalizadas com `ErrorDocument` (consulte `http://httpd.apache.org/docs-2.0/mod/core.html#errordocument`).

Índices
Caso nenhum documento `DirectoryIndex` seja encontrado, esse parâmetro permite ao Apache controlar a exibição de conteúdo do diretório.

Limite
Controla o acesso a um diretório ou a certos arquivos de clientes. As diretivas `Permitir`, `Negar` e `Ordenar` são usadas no interior de um arquivo `.htaccess` para essa finalidade. Sobre o uso dessas diretivas, consulte a documentação de módulos de acesso (`http://httpd.apache.org/docs-2.0/mod/mod_access.html`).

Opções
Permite o uso das diretivas `Opções` e `XBitHack` em um arquivo `.htaccess`. A diretiva `Opções` (`http://httpd.apache.org/docs-2.0/mod/core.html#options`) controla que recursos do servidor ficam disponíveis em um determinado diretório. A diretiva `XBitHack` (`http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack`) permite que arquivos com o conjunto de bits de execução sejam parcelados como SSI (consulte “"Server-Side Includes" com o `mod_include` ” (p 742)).

IMPORTANTE

Essas configurações são aplicadas recursivamente ao diretório atual e seus subdiretórios. Essas opções, exceto `Todos` e `Nenhum`, podem ser combinadas, separadas por espaços.

Exemplo 46.3 *LoadModule Diretiva*

```
<Diretório /srv/www/htdocs>
    AllowOverride Nenhum
</Directory>
<Diretório /srv/www/htdocs/project>
    AllowOverride Tudo
</Directory>
<Diretório /srv/www/htdocs/project/webapp>
    AllowOverride Índices Limite AuthConfig
</Directory>
```

AccessFileName *nomes de arquivos*

`AccessFileName` define o nome dos arquivos que podem substituir as permissões de acesso global e outras configurações de diretórios (consulte Diretório (p 724)).

A configuração padrão é `.htaccess`. Para declarar vários arquivos, separe-os com espaços.

Exemplo 46.4 *AccessFileName Diretiva*

```
AccessFileName .htaccess .acl permission.txt
```

ErrorLog *arquivo | "|comando"*

Especifica o nome do arquivo no qual o Apache registra as mensagens de erro. O Apache também pode fazer o registro em um comando ou script. A configuração padrão é `/var/log/apache2/error_log`.

Exemplo 46.5 *ErrorLog Diretiva*

```
ErrorLog /var/log/apache2/error_log
ErrorLog "|/path/to/script"
```

`LogLevel` *`nível`*

Isso define o nível de detalhamento das mensagens de registro a serem gravadas. Em ordem crescente de nível de detalhamento (e severidade decrescente das mensagens), o *`nível`* pode ser

- `emerg`
- `alerta`
- `crit`
- `erro`
- `aviso`
- `notificaç o`
- `info`
- `depurar`

A configuração padrão é `aviso`, recomendada para o funcionamento quotidiano. Para fins de depuração, `info` e `depurar` prestam informações úteis.

Exemplo 46.6 *LogLevel Diretiva*

```
LogLevel debug
```

Diretivas do Apache em /etc/apache2/httpd.conf: Seção dos hosts virtuais

Para manter diversos domínios ou nomes de host em uma máquina física, são necessários containers `VirtualHost`. Eles são declarados nas seções `Hosts Virtuais` da configuração. Para obter mais detalhes sobre a sintaxe e a funcionalidade dos hosts virtuais, consulte Seção 46.4, “Hosts virtuais” (p 737).

46.3.3 Ativando, iniciando e parando o Apache

Para ativar o servidor Web do Apache no momento da inicialização, use o editor de níveis de execução do YaST. Para iniciá-lo, selecione *Sistema → Serviços do Sistema (Nível de execução)* no YaST. Em seguida, navegue até a entrada *apache2*. Escolha *Habilitar* para que o Apache inicie automaticamente quando a máquina for inicializada. Convém aos usuários experientes usar a ferramenta `chkconfig` para executar a mesma tarefa na linha de comando: `/sbin/chkconfig -a apache2`.

Para iniciar ou parar o Apache, use o script `/usr/sbin/rcapache2` como o usuário `Root`. O script `/usr/sbin/rcapache2` utiliza os seguintes parâmetros para iniciar e parar o servidor Web do Apache:

`iniciar`
Inicia o servidor Web do Apache.

`startssl`
Inicia o servidor Web do Apache com o suporte a SSL. Para obter informações sobre a configuração do Apache com o SSL, consulte "Adicionando o suporte SSL" (p 728) e "Secure Socket Layer e o Apache: `mod_ssl`" (p 747).

`parar`
Pára o servidor Web do Apache.

`configtest`
Testa a configuração do Apache sem efetivamente parar, iniciar ou reiniciar o servidor Web. Como esse teste é forçado toda vez que o servidor é iniciado, recarregado ou reiniciado, normalmente não é necessário executar o teste explicitamente.

`reiniciar`
Primeiro pára e depois reinicia o servidor Web.

`try-restart`
Reinicia o servidor Web caso ele esteja em execução.

restart-hup
Reinicia o servidor Web do Apache enviando-o um sinal `SIGHUP`. Esse parâmetro normalmente não é usado.

normal e recarregar
Interrompe o servidor Web instruindo todos os processos bifurcados do Apache para primeiro concluir sua solicitação antes de encerrar. Com o término de cada processo, ele é substituído por um processo recém-iniciado, o que resulta na total "reinicialização" do Apache.

DICA

O `rcapache2 recarregar` é o método preferencial de reinicialização do Apache em ambientes de produção, pois permite que todos os clientes sejam atendidos sem provocar interrupções na conexão.

---

status
Verifica o status do tempo de execução do servidor Web do Apache.

Exemplo 46.7 *Exemplo: Saída ao iniciar e parar o Apache*

```
tux@sun # rcapache2 status
Verificando httpd2:                                    n o utilizado

tux@sun # rcapache2 configtest
Sintaxe OK

tux@sun # rcapache2 start
Iniciando httpd2 (pré-bifurcaç o)                      concluído

tux@sun # rcapache2 status
Verificando httpd2:                                    em execuç o

tux@sun # rcapache2 graceful
Recarregar httpd2 (reinicializaç o normal)             concluído

tux@sun # rcapache2 status
Verificando httpd2:                                    em execuç o
```

Um arquivo de configuração mal formulado pode fazer com que o Apache não inicie corretamente ou não inicie. Quando o Apache não iniciar, pode ser que não haja nem a exibição de uma mensagem. Sempre verifique o registro principal de erros de cada inicialização e reinicialização.

46.4 Hosts virtuais

O termo *host virtual* refere-se à habilidade do Apache de servir vários URIs (universal resource identifiers) a partir da mesma máquina física. Isso significa que vários domínios, como www.example.com e www.example.net, são executados por um servidor Web único em uma máquina física.

É prática comum usar hosts virtuais para evitar esforços administrativos (somente um servidor Web único precisa ser mantido) e despesas de hardware (não é necessário ter um servidor dedicado para cada domínio). Os hosts virtuais podem ser baseados em nome, IP ou porta.

Os hosts virtuais podem ser configurados através do YaST (consulte Host padrão (p 723)) ou através da edição manual da seção `Virtual Host` do `httpd.conf` (consulte a Seção 46.3.2, “Configurando o Apache manualmente” (p 728)).

Por padrão, o Apache no SUSE Linux está preparado para um arquivo de configuração por host virtual em `/etc/apache2/vhosts.d/`. Um modelo básico para um host virtual é fornecido neste diretório (`vhost.template`). A configuração de hosts virtuais também pode ser adicionada em outro local, por exemplo, em um arquivo que é então incluído na configuração.

IMPORTANTE

É muito útil verificar a configuração do host virtual com o comando `httpd2 -S`. Ele tem como saída as configurações de host virtual conforme entendido pelo Apache e pode ajudar você a ter certeza de que obterá os resultados esperados. Se você usar o Apache com sinalizadores como -DSSL, precisará usar os mesmos sinalizadores ao testar. Por exemplo, use `httpd2 -S -DSSL`.

46.4.1 Hosts virtuais baseados em nome

Com os hosts virtuais baseados em nome, mais de um site da Web é servido por endereço IP. O Apache usa o campo host no cabeçalho HTTP enviado pelo cliente para conectar a solicitação a uma entrada `ServerName` correspondente de uma das declarações do host virtual. Se não forem encontradas entradas `ServerName`, a primeira `VirtualHost` especificada será usada como padrão.

`NameVirtualHost` inicia a seção `Virtual Host` em uma configuração Apache.

NameVirtualHost

`NameVirtualHost` informa o servidor Web do Apache em qual endereço IP e, opcionalmente, em que porta escutar solicitações de clientes que contêm o nome de domínio no cabeçalho HTTP.

O primeiro argumento pode ser um nome de domínio completo, mas é recomendável usar o endereço IP. O segundo argumento é a porta e é opcional. Por padrão, a porta 80 é usada e é configurada através da diretiva `Listen` (Seleção de dispositivos de rede (p 721)).

O curinga `*` pode ser usado para que o endereço IP e a porta recebam solicitações em todas as interfaces. Os endereços IPv6 devem ser colocados entre colchetes.

Exemplo 46.8 *Variações de entradas VirtualHost baseadas em nome*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:164::]:80
```

<VirtualHost></VirtualHost> in the Name-Based Context

The `<VirtualHost></VirtualHost>` blocks holds the information that applies to a particular domain. When Apache receives a client request for a defined `VirtualHost`, it uses the directives enclosed in this section. Any Apache directive that is allowed in the `VirtualHost` context can be used here. The opening `VirtualHost` tag takes the following arguments in a name-based virtual host configuration:

- IP address (or fully qualified domain name) previously declared with the `NameVirtualHost` directive.
- Optional port number previously declared with the `NameVirtualHost` directive.

The wild card * is also allowed as a substitute for the IP address. This syntax is only valid in combination with the wild card usage in `NameVirtualHost *`. When using IPv6 addresses, the address must be included in square brackets.

Exemplo 46.9 *Name-Based VirtualHost Directives*

```
<VirtualHost 192.168.1.100:80>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.1.100:80>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin webmaster@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
    # 2002:c0a8:164:: is the IPv6 equivalent to 192.168.1.100
    ServerName www.example.org
    DocumentRoot /srv/www/htdocs/example.org
    ServerAdmin webmaster@example.org
    ErrorLog /var/log/apache2/www.example.org-error_log
    CustomLog /var/log/apache2/www.example.org-access_log common
</VirtualHost>
```

Neste exemplo, os domínios www.example.com e www.example.net são hospedados na máquina com o endereço IP `192.168.1.100`. O primeiro `VirtualHost` é o padrão para todas as solicitações de entrada ao servidor Web.

As diretivas `ErrorLog` (descritas na "`ErrorLog` *`arquivo | "|comando"`*" (p 733)) e `CustomLog` (consulte `http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog`) não precisam conter o nome de domínio. Aqui, use um nome de sua escolha.

46.4.2 Hosts virtuais baseados em IP

Esta configuração de host virtual alternativa requer a configuração de vários IPs para uma máquina. Uma instância do Apache hospeda vários domínios, a cada qual é atribuído um IP diferente.

IMPORTANTE: Endereços IP e hosts virtuais baseados em IP

O servidor físico deve ter um endereço IP para cada host virtual baseado em IP. Se a máquina não tiver várias placas de rede, interfaces de rede virtuais (criação de álias de IP) também poderão ser usadas.

Configurando a criação de álias de IP

Para que o Apache hospede vários IPs, a máquina física deve aceitar solicitações para vários IPs. Isto é chamado de hospedagem de vários IPs. Além disso, a criação de álias de IP deve estar ativada no kernel. Esta é a configuração padrão no SUSE Linux.

Uma vez que o kernel foi configurado para a criação de álias de IP, os comandos `ifconfig` e `route` podem ser usados para configurar IPs adicionais no host. Esses comandos devem ser executados como `root`.

No exemplo a seguir, pressupõe-se que o host já tenha o IP `192.168.0.10` atribuído para o dispositivo de rede `eth0`. Digite o comando `ifconfig` para exibir o IP do host. Mais endereços IP podem ser adicionados com os seguintes comandos:

```
ip addr add 192.168.0.20/24 dev eth0
ip addr add 192.168.0.30/24 dev eth0
```

Todos estes endereços IP são atribuídos ao mesmo dispositivo de rede física (`eth0`).

`<VirtualHost></VirtualHost>` no contexto baseado em IP

Uma vez que a criação de álias de IP foi configurada no sistema (ou o host foi equipado com várias placas de rede), o Apache pode ser configurado. É necessário um bloco separado `VirtualHost` para cada servidor virtual.

O seguinte exemplo mostra o Apache sendo executado em uma máquina com o IP `192.168.1.10`, hospedando dois domínios nos IPs adicionais `192.168.0.20` e `192.168.0.30`. Este exemplo particular somente funciona em uma rede privada, pois os IPs de `192.168.0.0` a `192.168.0.255` não são roteados à Internet pública.

Exemplo 46.10 *DiretivasVirtualHost baseadas em IP*

```
<VirtualHost 192.168.0.20>
    ServerName www.example.com
    DocumentRoot /srv/www/htdocs/example.com
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com-error_log
    CustomLog /var/log/apache2/www.example.com-access_log common
</VirtualHost>

<VirtualHost 192.168.0.30>
    ServerName www.example.net
    DocumentRoot /srv/www/htdocs/example.net
    ServerAdmin tux@example.net
    ErrorLog /var/log/apache2/www.example.net-error_log
    CustomLog /var/log/apache2/www.example.net-access_log common
</VirtualHost>
```

Aqui, diretivas `VirtualHost` somente são especificadas para interfaces que não sejam `192.168.0.10`. Quando uma diretiva `Listen` (descrita em Seleção de dispositivos de rede (p 721)) também é configurada para `192.168.0.10`, um host virtual baseado em IP separado deve ser criado para responder solicitações HTTP àquela interface, caso contrário as diretivas encontradas na seção `Servidor Principal` do `/etc/apache2/httpd.conf` (consulte a “Diretivas do Apache em /etc/apache2/httpd.conf: Servidor principal ” (p 731)) serão aplicadas.

46.5 Módulos do Apache

O software do Apache é criado de uma maneira modular: toda a funcionalidade exceto algumas tarefas centrais são manipuladas por módulos. Isso progrediu tanto que até o HTTP é processado por um módulo (http_core).

Os módulos do Apache podem ser compilados no Apache binário no momento da construção ou dinamicamente carregados durante a execução. Para o carregamento durante a execução, consulte a “`LoadModule` *`module_identifier /path/to/module`* ” (p 730) para carregar módulos manualmente e Módulos (p 722) para usar o YaST.

O Apache no SUSE Linux vem com os seguintes módulos já disponíveis no RPM `apache2` (prefixo "mod_" omitido aqui): access, actions, alias, asis, auth, auth_anon, auth_dbm, auth_digest, auth_ldap, autoindex, cache, case_filter, case_filter_in, cern_meta, cgi, charset_lite, dav, dav_fs, deflate, dir, disk_cache, dumpio, echo, env, expires, ext_filter, file_cache, headers, imap, include, info, ldap, log_config,

log_forensic, logio, mem_cache, mime, mime_magic, negotiation, proxy, proxy_connect, proxy_ftp, proxy_http, rewrite, setenvif, speling, ssl, status, suexec, unique_id, userdir, usertrack e vhost_alias. Além disso, o SUSE Linux fornece os seguintes módulos do Apache como pacotes RPM que precisam ser instalados separadamente: `apache2-mod_auth_mysql`, `apache2-mod_fastcgi`, `apache2-mod_macro`, `apache2-mod_murka`, `apache2-mod_perl`, `apache2-mod_php4`, `apache2-mod_php5`, `apache2-mod_python` e `apache2-mod_ruby`.

Alguns desses módulos são documentados com mais detalhes nesta seção. Para obter uma descrição de outros módulos na distribuição base, consulte o site de Módulos do Apache na Web em `http://httpd.apache.org/docs-2.0/mod/`. Para módulos de terceiros, consulte `http://modules.apache.org/`.

Os módulos do Apache podem ser divididos em três categorias diferentes: módulos base, módulos de extensão e módulos externos.

46.5.1 Módulos de base

Os módulos de base são compilados no Apache por padrão. Eles ficam disponíveis, a menos que sejam explicitamente deixados de fora no momento da construção. O Apache do SUSE Linux possui somente a compilação dos módulos de base mínimos, mas todos eles estão disponíveis como *objetos compartilhados*: em vez de serem incluídos no próprio binário `/usr/sbin/httpd2`, eles podem ser incluídos durante a execução configurando-se `APACHE_MODULES` em `/etc/sysconfig/apache2`.

"Server-Side Includes" com o `mod_include`

O `mod_include` oferece um método de processamento de arquivos antes do envio de dados para o cliente. Normalmente, o `mod_include` é usado para a inclusão de arquivos em um documento. Esses arquivos, por sua vez, são analisados como HTML antes de chegar até o cliente. É por isso que é chamado de "server-side includes" (SSI).

Com os SSIs, comandos especiais são executados no servidor, acionados por comentários SGML formatados. Esses comandos SGML possuem a seguinte sintaxe:

```
<!--#element attribute=value -->
```

Para obter uma lista de valores de *elementos* e *atributos*, consulte a documentação mod_include em http://httpd.apache.org/docs-2.0/mod/mod_include.html.

Para usar o mod_include no SUSE Linux, adicione include a APACHE_MODULES em /etc/sysconfig/apache2 ou use o YaST de acordo com a descrição em Módulos (p 722).

DICA

Use a diretiva XBitHack (http://httpd.apache.org/docs-2.0/mod/mod_include.html#xbithack) para instruir o Apache a analisar arquivos com o conjunto de bits executar das diretivas SSI.

Isso significa que, em vez de ter de mudar a extensão de um arquivo para marcá-lo como portador de elementos SSI (.shtml no exemplo acima), você pode usar um arquivo .html normal e executar chmod +x *myfile*.html.

Interface de Gateway Comum: mod_cgi

O mod_cgi permite ao Apache entregar conteúdos criados por programas ou scripts de CGI externos ("Interface de Gateway Comum"). Ele atua como uma instância entre uma linguagem de programação disponível na máquina física e o servidor Web do Apache. Teoricamente, os scripts CGI podem ser escritos em qualquer linguagem de programação. Em geral, são usadas linguagens como Perl ou C. mod_cgi é a forma mais comum de incluir conteúdo dinâmico em um site.

A programação CGI difere da programação "normal" no sentido de que os programas e scripts CGI precisam ser capazes de gerar um tipo MIME Content-type: text/html para produzir em HTML.

Exemplo 46.11 *Um script CGI simples em Perl*

```
#!/path/to/perl
print "Content-type: text/html\n\n";
print "Hello, World.";
```

A diferença entre os módulos especificamente atrelados a uma linguagem de programação (como mod_php5) e mod_cgi reside na possibilidade de se combinar mod_cgi com mod_suexec (consulte “Executando as CGIs como um usuário

diferente com mod_suexec " (p 745)). Essa combinação permite que os scripts CGI sejam executados com um ID de usuário. Em geral, os scripts que usam o mod_cgi isoladamente ou o mod_php5 são executados com o ID do usuário Apache (padrão no SUSE Linux: wwwrun). Os módulos projetados para uma linguagem de programação (como mod_php5 ou mod_ruby) embutem um interpretador persistente no Apache para executar scripts com o ID de usuário do Apache.

Em decorrência disso, as CGIs com mod_suexec ajudam com a clareza administrativa já que os processos CGI podem ser designados a usuários específicos em vez do próprio servidor Web. Além disso, essa combinação propicia uma melhor segurança do sistema de arquivos: o script herda somente os direitos do sistema de arquivos do usuário. No caso contrário dos módulos, o script recebe as permissões de arquivo do usuário do servidor Web, que podem levar à visibilidade não desejada de dados no sistema de arquivos.

Os CGIs são encerrados quando a solicitação de um cliente ao servidor Web termina. Isso significa que as CGIs não são persistentes e liberam todos os recursos ocupados após o encerramento. Trata-se de uma vantagem, sobretudo em caso de programação incorreta. Com os módulos, os efeitos dos erros de programação podem se acumular, pois o interpretador é persistente. Isso pode acarretar uma falha na liberação dos recursos, como conexões de bancos de dados, e pode exigir que o Apache seja reiniciado.

Para usar o mod_cgi no SUSE Linux, adicione cgi a APACHE_MODULES em /etc/sysconfig/apache2 ou use o YaST de acordo com a descrição em Módulos (p 722). O diretório padrão das CGIs no SUSE Linux é /srv/www/cgi-bin/.

Se estiver fazendo a edição manual do arquivo de configuração do Apache, use esse exemplo como uma diretriz para a configuração de mod_cgi.

Exemplo 46.12 *Ativação manual de mod_cgi*

```
# Global Environment
LoadModule cgi_module /path/to/mod_cgi.so

# Servidor principal e/ou do host virtual e/ou
# Diretório e/ou contexto .htaccess
AddHandler cgi-script .cgi .pl

# Contexto do servidor principal e/ou do host virtual
ScriptAlias /cgi-bin/ /srv/www/cgi-bin/

# Outra opç o é permitir explicitamente os scripts CGI em um diretório
# Contexto do servidor principal e/ou host virtual
<Diretório /srv/www/some/dir>
    Opções +ExecCGI
<Diretório>
```

46.5.2 Módulos de extensão

Em geral, os módulos chamados de extensões vêm no pacote de software Apache, mas normalmente não são compilados estaticamente no servidor. No SUSE Linux, esses módulos estão disponíveis como objetos compartilhados que podem ser carregados no Apache durante a execução.

Executando as CGIs como um usuário diferente com `mod_suexec`

Em combinação com `mod_cgi` (“Interface de Gateway Comum: `mod_cgi` ” (p 743)), o `mod_suexec` permite que os scripts CGI sejam executados como um usuário e grupo especificados. O programa suEXEC, localizado em `/usr/sbin/suexec2`, é usado para essa finalidade. Trata-se de um agrupador chamado pelo Apache toda vez que um script ou programa CGI é executado. Em seguida, o agrupador e o programa fazem a designação do usuário e ID de grupo configurados. Em decorrência disso, ele é executado como o usuário ou grupo configurado.

Embora essa abordagem reduza bastante o risco de segurança associado aos scripts CGI gerados pelo usuário, ela também suscita algumas considerações importantes:

Considerações para o uso de suEXEC

- `suEXEC docroot`—Toda execução de scripts fica limitada a esse diretório de base. Isso significa que a execução de scripts com o suexec fora de `docroot` não é possível e resulta em erro. `docroot` é definido no momento da compilação de `suEXEC` e não pode ser mudado durante a execução. O padrão no SUSE Linux é `/srv/www`.

- `uidmin`—Esse script representa o ID mínimo que um usuário precisa ter para executar scripts com `suEXEC`. Assim, evita-se que os scripts sejam executados como usuários do sistema, como `root`. Não crie usuários com um ID abaixo de `uidmin` caso eles devam ser usados com `mod_suexec`. O `uidmin` padrão no SUSE Linux é 96.

- `gidmin`—Trata-se do mesmo conceito que `uidmin`, mas para o ID de grupo. O `gidmin` padrão no SUSE Linux é 96.

- Permissões de Diretório e Arquivo—O script em questão precisa ser propriedade do mesmo usuário e pertencer ao mesmo grupo de acordo com a especificação de usuário ou grupo `suEXEC`. Além disso, o arquivo não pode ser gravável por ninguém, exceto o proprietário. O diretório onde o script se situa também deve ser gravável somente pelo proprietário.

- `suEXEC safepath`—Todos os programas usados em um script (como o Perl) precisam estar localizados nos caminhos considerados seguros para o suexec. `safepath` é definido no momento da compilação do `suEXEC` e não pode ser mudado durante a execução. O `safepath` padrão no SUSE Linux é `/usr/local/bin:/usr/bin:/bin`.

Em caso de erros causados por `mod_suexec`, consulte o arquivo de registro suexec em `/var/log/apache2/suexec.log`.

Para usar o `mod_suexec` no SUSE Linux, adicione `suexec` a `APACHE_MODULES` em `/etc/sysconfig/apache2` ou use o YaST de acordo com a descrição em Módulos (p 722). Lembre-se que é necessário o `mod_cgi` para executar o suexec.

A melhor forma de usar o `mod_suexec` é aplicando-o em um ambiente de host virtual, descrito em Seção 46.4, “Hosts virtuais” (p 737). Para especificar um determinado usuário e grupo como o que irá executar os scripts CGI, use a seguinte sintaxe no arquivo portador das declarações do host virtual (o padrão no SUSE Linux é `/etc/apache2/vhosts.d/*`):

Exemplo 46.13 *mod_suexec Configuração*

```
<VirtualHost 192.168.0>
# ...
ScriptAlias /cgi-bin/ /srv/www/vhosts/www.example.com/cgi-bin/
SuexecUserGroup tux users
# ...
</VirtualHost>
```

A sintaxe `SuexecUserGroup` *`nome de usuário grupo`* deste exemplo designa a todos os scripts contidos em `/srv/www/vhosts/www.example.com/cgi-bin/` o ID de usuário de tux e o ID de grupo dos usuários.

Secure Socket Layer e o Apache: `mod_ssl`

`mod_ssl` oferece uma criptografia forte usando protocolos de secure sockets layer (SSL) e segurança de camada de transporte (TLS) para a comunicação HTTP entre um cliente e o servidor Web. Para isso, o servidor envia um certificado SSL contendo informações que comprovam a validade da identidade do servidor antes que solicitações a um URL sejam respondidas. Por sua vez, isso garante que o servidor é o único ponto de terminação correto para essa comunicação. Além disso, o certificado gera uma conexão criptografada entre o cliente e o servidor capaz de transmitir informações sem o risco de exposição de conteúdo confidencial em texto simples. O efeito mais visível do uso de `mod_ssl` com o Apache é que os URLs aparecem com o prefixo `https://` em vez do prefixo `http://`.

A porta padrão das solicitações SSL e TLS no servidor Web é a 443. Não há conflito entre uma recepção “normal” do Apache na porta 80 e uma recepção habilitada por SSL/TLS do Apache na porta 443. Na verdade, HTTP e HTTPS podem ser executados com a mesma instância do Apache. Geralmente, um host virtual (consulte Seção 46.4, “Hosts virtuais” (p 737)) é usado para encaminhar solicitações à porta 80 e à porta 443 para servidores virtuais separados.

IMPORTANTE: Hosts virtuais baseados em nome e SSL

É impossível executar vários hosts virtuais habilitados por SSL em um servidor dotado de apenas um endereço IP. Os usuários que se conectarem a uma configuração como essa receberão uma mensagem de aviso informando que o certificado não corresponde ao nome do servidor toda vez que eles visitam o URL. Um endereço IP ou porta separado é necessário para todo domínio habilitado por SSL para efetivar a comunicação baseada em um certificado SSL válido.

Apesar da mensagem de aviso, ainda assim você obterá o mesmo nível de criptografia que teria em qualquer site SSL válido. Isso significa que, contanto que a mensagem de aviso seja aceitável, a comunicação entre o servidor Web e o cliente continua segura. O conceito de conhecimento único da identidade do servidor, que é garantido por um certificado SSL válido, é perdido.

Para ativar o `mod_ssl` no SUSE Linux, adicione `ssl` a `APACHE_MODULES` em `/etc/sysconfig/apache2` ou use o YaST de acordo com a descrição em Módulos (p 722). Além disso, o servidor Web precisa estar configurado para fazer a recepção na porta 443 de padrão HTTPS. Isso pode ser feito manualmente em `/etc/apache2/listen.conf` ou em YaST por meio da entrada de menu *Recepção* (consulte Seleção de dispositivos de rede (p 721)).

Para criar um certificado SSL de teste, digite `cd /usr/share/doc/packages/apache2; ./certificate.sh` como a `raiz`. Siga as instruções na tela para compor o certificado SSL. Os arquivos de certificado resultantes são abrigados nos diretórios `/etc/apache2/ssl*`.

Um certificado “real” com validade global pode ser obtido com fornecedores como Thawte (`http://www.thawte.com/` ou Verisign (`www.verisign.com`).

Se estiver fazendo a edição manual do arquivo de configuração do Apache, use esse exemplo como uma diretriz para a configuração de `mod_ssl`.

Exemplo 46.14 *Configuração manual de mod_ssl*

```
# Ambiente Global
# faça a recepç o na porta SSL padr o
Recepç o 443
# carregue o módulo somente se rcapache2 start-ssl tiver sido emitido
<IfDefine SSL>
LoadModule ssl_module /path/to/mod_ssl.so
</IfDefine>

# Contexto do servidor principal
# incluir configuraç o SSL global (em todo o servidor)
# que n o seja especifica a algum host virtual
# somente se ssl_module tiver sido carregado
<IfModule mod_ssl.c>
Include /etc/apache2/ssl-global.conf
</IfModule>
```

DICA

Não se esqueça de abrir o firewall do Apache habilitado por SSL na porta 443. Para fazer isso por meio do YaST, vá até *Segurança e Usuários* → *Firewall* → *Serviços Permitidos*. Em seguida, adicione *Servidor HTTPS* à lista de *Serviços Permitidos*.

46.5.3 Módulos externos

Oficialmente, os módulos rotulados como externos não estão incluídos na distribuição do Apache. No entanto, o SUSE Linux oferece vários deles já disponíveis para uso. Este capítulo explica brevemente alguns módulos externos e sua funcionalidade.

Usando o Perl para gerenciar o Apache: `mod_perl`

O `mod_perl` embute um interpretador Perl persistente no Apache. Isso evita a sobrecarga causada por um `mod_cgi` que chama um executável externo em cada solicitação a um CGI. O `mod_perl` também permite controlar vários aspectos da funcionalidade do Apache com a ajuda da linguagem de programação Perl.

Para usar o `mod_perl` no SUSE Linux, instale o RPM `apache2-mod_perl` e ative o módulo através do YaST (Módulos (p 722)) ou manualmente no `/etc/sysconfig/apache2`. Após a instalação e ativação, um arquivo de configuração separado, `mod_perl.conf`, é colocado em `/etc/apache2/conf.d/`. Adicionalmente, o script

de inicialização mod_perl é instalado como mod_perl-startup.pl. Para obter mais informações sobre como usar o módulo, consulte a documentação disponível no site mod_perl na Web (http://perl.apache.org/).

Servindo o PHP: mod_php4, mod_php5

O PHP é uma linguagem de programação conhecida direcionada originalmente ao uso na Web. Ele existe em duas versões: PHP4 e PHP5. Enquanto o PHP4 representa o conceito e a abordagem clássicos do PHP, o PHP5 introduziu novas possibilidades de programação orientada a objetos junto com vários outros recursos avançados. O mod_php4 e o mod_php5 estão disponíveis no SUSE Linux. Eles embutem o interpretador PHP no Apache como um módulo persistente.

Para usar o mod_php4 ou mod_php5 no SUSE Linux, instale o respectivo RPM (apache2-mod_php4, apache2-mod_php5) e ative o módulo por meio do YaST (Módulos (p 722)) ou manualmente, no /etc/sysconfig/apache2.

Após a instalação e a ativação, um arquivo de configuração separado para o respectivo módulo (php4.conf ouphp5.conf) é colocado em /etc/apache2/conf.d/. O site do PHP na Web (http://www.php.net) é um recurso excelente para usar o Apache junto com o PHP.

Python e Apache: mod_python

O mod_python embute o interpretador Python no Apache. Python é uma linguagem de programação orientada a objetos com uma sintaxe muito clara e legível. Um recurso incomum, porém conveniente, é que a estrutura do programa depende da indentação do código-fonte e não de elementos de demarcação regulares como begin e end.

Para usar o mod_python no SUSE Linux, instale o RPM apache2-mod_python e ative o módulo por meio do YaST (Módulos (p 722)) ou manualmente, no /etc/sysconfig/apache2. Para obter mais informações sobre como usar o módulo, consulte a documentação disponível no site mod_python na Web (http://www.modpython.org/).

Interpretador Ruby no Apache: mod_ruby

O mod_ruby embute o interpretador Ruby no servidor Web Apache, permitindo que os scripts CGI Ruby sejam executados de forma nativa. Ruby é uma linguagem de programação de alto nível orientada a objetos relativamente nova que lembra certos aspectos do Perl e Python. Como o Python, ela possui uma sintaxe limpa e transparente. Por outro lado, o Ruby adotou abreviações (como $.r para o número da última linha lida no arquivo de entrada) que são apreciadas por alguns programadores, mas não por outros. O conceito básico do Ruby é muito parecido com o do Smalltalk.

Para usar o mod_ruby no SUSE Linux, instale o RPM apache2-mod_ruby e ative o módulo por meio do YaST (Módulos (p 722)) ou manualmente, no /etc/sysconfig/apache2. Para obter mais informações sobre como usar o módulo, consulte a documentação disponível no site mod_ruby na Web (http://www.modruby.net/en/index.rbx).

Acesso ao sistema de arquivos nativos: mod_dav

O mod_dav oferece a funcionalidade WebDAV (Web-Based Distributed Authoring and Versioning) para o Apache. WebDAV é uma extensão do protocolo HTTP que permite que os usuários editem e gerenciem arquivos em colaboração em servidores remotos. Os recursos do WebDAV são semelhantes aos do FTP, com a diferença principal que o HTTP é usado como o protocolo subjacente para acesso ao servidor. Na verdade, o mod_dav faz com que um servidor Web Apache seja um sistema avançado de arquivos remotos.

É uma boa prática, se não for necessário, limitar o acesso aos diretórios disponíveis por meio do WebDAV. As precauções mínimas a serem tomadas são configurar a autenticação básica HTTP para o recurso WebDAV e possuir condições Limit dentro de uma diretiva Location.

Para acessar um recurso WebDAV, o software compatível com WebDAV precisa estar presente no cliente. O SUSE Linux já é fornecido com recursos WebDAV: Konqueror com o prefixo webdav:// ou webdavs:// (para WebDAV em conexões SSL) pode ser usado para conectar-se a um sistema de arquivos WebDAV do Apache.

O mod_dav requer o módulo mod_dav_fs, que oferece acesso ao sistema de arquivos real para o WebDAV. Para usar o mod_dav no SUSE Linux, ative o módulo por meio do YaST (Módulos (p 722)) ou manualmente, no /etc/sysconfig/apache2. Faça

o mesmo para o mod_dav_fs. Para obter mais informações sobre como usar o módulo, consulte a documentação disponível no site mod_dav na Web (http://httpd.apache.org/docs-2.0/mod/mod_dav.html).

Oferecendo home pages do usuário: mod_userdir

O padrão do mod_userdir no SUSE Linux é oferecer o conteúdo de cada pasta ~/public_html do usuário como páginas da Web públicas. O URL para acessar essas páginas é http://www.exemplo.com/~*nome_de_usuário*/.

DICA

O mod_userdir no SUSE Linux proíbe o acesso a quaisquer diretórios do diretório pessoal do usuário root por questões de segurança. Você também pode permitir especificamente que somente certos usuários tenham home pages públicas usando:

```
# Main server context
UserDir disabled
UserDir enabled tux wilber
```

Para usar o mod_userdir no SUSE Linux, ative o módulo por meio do YaST (Módulos (p 722)) ou manualmente, no /etc/sysconfig/apache2. Para obter mais informações sobre como usar o módulo, consulte a documentação disponível no site mod_userdir na Web (http://httpd.apache.org/docs-2.0/mod/mod_userdir.html).

Mudando o layout do URL: mod_rewrite

O mod_rewrite é geralmente conhecido como "o canivete suíço da manipulação de URL". Ele regrava URLs solicitados dinamicamente com base em um conjunto de regras especificado. O resultado geralmente é semelhante a http://www.exemplo.com/2/1/de para http://www.exemplo.com/display.php?cat=2&article=1&lang=de.

O URL Rewriting Guide (Guia de regravaç o de URL) explica as vantagens e desvantagens do módulo avançado e complexo:

“Com o mod_rewrite, ou você dá um tiro no próprio pé na primeira vez e nunca o usa novamente ou o adora para o resto de sua vida devido a sua capacidade.”

Os conjuntos `RewriteRule` podem ser definidos em todos os contextos de configuração: para o servidor principal, para hosts virtuais, para diretórios e para arquivos `.htaccess`. Um bom ponto de partida para a regravação de URLs com o `mod_rewrite` é o URL Rewriting Guide (Guia de regravação de URL) em `http://httpd.apache.org/docs-2.0/misc/rewriteguide.html`.

Para usar o `mod_rewrite` no SUSE Linux, ative o módulo por meio do YaST (Módulos (p 722)) ou manualmente, no `/etc/sysconfig/apache2`.

46.6 Segurança

Um servidor Web exposto à Internet pública requer um esforço administrativo contínuo. É inevitável que sejam levantadas questões de segurança, relacionadas tanto ao software como à configuração incorreta acidental. Aqui vão algumas dicas sobre como lidar com elas.

Mantendo-se atualizado

Se forem encontradas vulnerabilidades no software Apache, um aviso de segurança será emitido pelo SUSE. Ele contém instruções para a correção de vulnerabilidades, que devem ser aplicadas o mais rápido possível. A lista de discussão sobre anúncios de segurança do SUSE está disponível em `http://www.suse.com/us/private/support/online_help/mailinglists/`. As informações mais recentes sobre questões de segurança dos pacotes do SUSE Linux também estão disponíveis online em `http://www.novell.com/linux/security/securitysupport.html`.

Além disso, você pode inscrever-se na lista de discussão sobre anúncios do Apache (`http://httpd.apache.org/lists.html#http-announce`) onde são publicadas novas versões e correções de erros.

Permissões do DocumentRoot

Por padrão, no SUSE Linux, o diretório `DocumentRoot` `/srv/www/htdocs` e o diretório CGI `/srv/www/cgi-bin` pertencem ao usuário`root`. Não mude essas permissões. Se os diretórios fossem graváveis para todos, qualquer usuário poderia colocar arquivos neles. Esses arquivos seriam então executados pelo Apache

com as permissões de `wwwrun` que poderiam dar ao usuário acesso não desejado a recursos do sistema de arquivos. Use subdiretórios de `/srv/www/htdocs` e `/srv/www/cgi-bin` para organizar dados específicos do usuário ou domínio em combinação com a diretiva `Directory` (consulte Diretório (p 724)).

Diretórios CGI e SSI

Os scripts interativos em Perl, PHP, SSI ou qualquer outra linguagem de programação podem essencialmente executar comandos arbitrários. Limitar a execução de CGIs e SSIs (consulte a “Interface de Gateway Comum: `mod_cgi` ” (p 743), o Álias de script (p 725) e a “"Server-Side Includes" com o `mod_include` ” (p 742)) a diretórios específicos em vez de permiti-los globalmente é uma opção para diminuir o risco.

Outra possibilidade é trabalhar com o `mod_suexec` (consulte a “Executando as CGIs como um usuário diferente com `mod_suexec` ” (p 745)) para CGIs em geral. Para os módulos Apache, uma configuração segura para os interpretadores, como descrito na “Servindo o PHP: `mod_php4`, `mod_php5` ” (p 750), ajuda a manter o ambiente da Web seguro.

Permissões de acesso

Muitas vezes, principalmente em ambientes de teste, permissões de acesso a um servidor Web são tratadas casualmente devido à natureza do teste de uma configuração. Isso pode resultar na revelação acidental de informações confidenciais ou mesmo na exposição de um servidor inteiro ao público errado. Use a diretiva `Order` (`http://httpd.apache.org/docs-2.0/mod/mod_access.html#order`) em combinação com arquivos `.htaccess` (consulte a “`AccessFileName` *`nomes de arquivos`* ” (p 733)) para permitir acesso a certos sites da Web somente para usuários ou clientes específicos.

Você também pode usar a abordagem “segurança por ofuscação”: um exemplo típico disso é executar o Apache em uma porta não-padrão (consulte Seleção de dispositivos de rede (p 721)). Isso resulta em URLs com a porta anexada, como `http://www.example.com:8765`, que é aceitável em ambientes de teste.

46.7 Solução de problemas

Se o Apache não for iniciado, a página da Web não estiver acessível ou os usuários não puderem se conectar ao servidor Web, é importante encontrar a causa do problema. A

seguir, estão alguns locais típicos para procurar por explicações de erros e coisas importantes a serem verificadas.

Primeiro, o `rcapache2` (descrito na Seção 46.3.3, “Ativando, iniciando e parando o Apache” (p 735)) mostra detalhes sobre erros, portanto pode ser bastante útil se for realmente usado para operar o Apache. Algumas vezes, é tentador usar o `/usr/sbin/httpd2` binário para iniciar ou interromper o servidor Web. Evite fazer isso e use o script `rcapache2`. O `rcapache2` fornece até dicas sobre como resolver erros de configuração.

Segundo, a importância de arquivos de registro (consulte a “Arquivos de registro” (p 719)) não pode ser demasiadamente enfatizada. No caso de erros fatais e não fatais, deve-se procurar as causas nos arquivos de registro do Apache. Você também pode controlar o detalhamento das mensagens registradas com a diretiva `LogLevel` (consulte a “`LogLevel` *`nível`* ” (p 734)) se forem necessários mais detalhes nos arquivos de registro.

DICA

Observe as mensagens de registro do Apache com o comando `tail -F /var/log/apache2/*_log &`. A seguir, execute `rcapache2 restart`. Agora, tente conectar-se a um navegador e verifique a saída.

Um erro comum é não abrir as portas do Apache na configuração de firewall do servidor. Se você configura o Apache com o YaST, existe uma opção separada disponível que cuida desta questão específica .

Se o erro não puder ser descoberto com a ajuda de qualquer desses meios, verifique o banco de dados de erros do Apache online em `http://httpd.apache.org/bug_report.html`. A comunidade de usuários do Apache também pode ser acessada através de uma lista de discussão disponível em `http://httpd.apache.org/userslist.html`. Um grupo de discussão recomendado é `comp.infosystems.www.servers.unix`.

46.8 Para obter mais informações

Apache é um servidor Web amplamente utilizado. Como conseqüência, existem muitos sites da Web que oferecem suporte e ajuda a ele com diferentes níveis de qualidade.

Em qualquer caso, o ponto de partida para qualquer pesquisa sobre o Apache e suas possibilidades deve ser http://httpd.apache.org/docs-2.0/.

Além disso, o pacote RPM apache2-doc contém o manual do Apache para instalação e referência local. Para obter algumas dicas de configuração específicas do SUSE, o arquivo /usr/share/doc/packages/apache2 contém uma referência rápida.

O pacote RPM apache2-example-pages contém algumas páginas de exemplo para o Apache que mostram informações sobre o servidor Web.

46.8.1 Módulos do Apache

Mais informações sobre os módulos externos do Apache do Seção 46.5.3, “Módulos externos” (p 749) estão disponíveis nos seguintes locais:

- httpd.apache.org/docs-2.0/mod/
- http://www.php.net/manual/en/install.unix.apache2.php
- http://www.modpython.org/
- http://www.modruby.net/
- http://perl.apache.org/

46.8.2 CGI

Mais informações sobre o uso do mod_cgi (consulte “Interface de Gateway Comum: mod_cgi ” (p 743)) e da programação CGI estão disponíveis nos seguintes locais:

- http://www.modperl.com/
- http://www.modperlcookbook.org/
- http://www.fastcgi.com/
- http://www.boutell.com/cgic/

46.8.3 Fontes diversas:

Se você tiver dificuldades específicas ao Apache no SUSE Linux, consulte o Banco de Dados de Suporte SUSE em http://portal.suse.com/sdb/en/index.html.

O histórico do Apache pode ser encontrado em http://httpd.apache.org/ABOUT_APACHE.html. Essa página também explica porque o servidor é chamado de Apache.

As informações sobre o upgrade da versão 1.3 para a versão 2.0 estão disponíveis em http://httpd.apache.org/docs-2.0/en/upgrading.html.

47 Sincronização de arquivos

Atualmente, muitas pessoas usam vários computadores; um computador em casa, um ou mais no trabalho e possivelmente um laptop ou PDA quando viajam. Vários arquivos são necessários em todos esses computadores. Talvez você queira trabalhar com todos os computadores e modificar os arquivos, conseqüentemente tendo a versão mais recente dos dados disponíveis em todos os computadores.

47.1 Software de sincronização de dados disponível

A sincronização de dados não é um problema para computadores permanentemente conectados por uma rede rápida. Nesse caso, use um sistema de arquivos de rede, como o NFS, e armazene os arquivos em um servidor para que todos os hosts acessem os mesmos dados via rede. Essa abordagem será impossível se a conexão de rede for instável ou não permanente. Quando você viaja com um laptop, precisa ter cópias de todos os arquivos necessários no disco rígido local. Entretanto, é necessário sincronizar os arquivos modificados. Quando você modificar um arquivo em um computador, verifique se uma cópia dele foi atualizada em todos os outros computadores. No caso de cópias ocasionais, elas podem ser feitas manualmente com o scp ou o rsync. Entretanto, se vários arquivos forem envolvidos, o procedimento poderá ser complicado e demandar muito cuidado para evitar erros, como a sobregravação de um arquivo novo por um antigo.

ATENÇÃO: Risco de perda de dados

Antes de começar a gerenciar seus dados com um sistema de sincronização, você deve se informar sobre o programa usado e testar sua funcionalidade. É indispensável ter um backup de arquivos importantes.

A tarefa prolongada e sujeita a erros de sincronizar dados manualmente pode ser evitada se você usar um dos programas que utilizam vários métodos para automatizá-la. Os resumos a seguir têm o simples objetivo de dar uma visão geral sobre como esses programas funcionam e como podem ser usados. Se você planeja usá-los, leia a documentação do programa.

47.1.1 Unison

O Unison não é um sistema de arquivos de rede. Em vez disso, os arquivos são simplesmente gravados e editados localmente. O programa Unison pode ser executado manualmente para sincronizar arquivos. Quando a sincronização é executada pela primeira vez, um banco de dados é criado nos dois hosts, contendo checksums, marcações de horários e permissões dos arquivos selecionados. Na próxima vez em que for executado, o Unison poderá reconhecer quais arquivos foram mudados e propor que a transmissão seja feita do outro host ou para ele. Normalmente, todas as sugestões podem ser aceitas.

47.1.2 CVS

O CVS, que é mais usado para gerenciar versões de origem de programas, oferece a possibilidade de manter cópias dos arquivos em vários computadores. Dessa forma, ele também é adequado para sincronização de dados. O CVS mantém um repositório central no servidor, no qual os arquivos e as mudanças feitas neles são gravados. As mudanças realizadas localmente são enviadas para o repositório e podem ser recuperadas de outros computadores por meio de uma atualização. Todos os procedimentos devem ser iniciados pelo usuário.

O CVS é muito suscetível a erros quando ocorrem mudanças em vários computadores. As mudanças são fundidas e, se elas forem feitas nas mesmas linhas, um conflito será reportado. Quando ocorre um conflito, o banco de dados permanece em estado consistente. O conflito só fica visível para resolução no host cliente.

47.1.3 subversion

Ao contrário do CVS, cuja subversão "desenvolvida" é um projeto de design consistente, o subversion foi desenvolvido como sucessor tecnicamente apropriado do CVS.

O subversion foi aprimorado em vários aspectos com relação ao seu predecessor. Devido ao seu histórico, o CVS mantém apenas arquivos e não lida com diretórios. Os diretórios também podem ter um histórico de versão no subversion e podem ser copiados e renomeados, assim como os arquivos. Também é possível adicionar metadados a todos os arquivos e todos os diretórios. Esses metadados podem ser totalmente mantidos com o controle de versão. Em oposição ao CVS, o subversion suporta o acesso transparente à rede em protocolos dedicados, como o WebDAV. O WebDAV estende a funcionalidade do protocolo HTTP para permitir acesso de gravação colaborativo a arquivos em servidores Web remotos.

O subversion foi amplamente agrupado com base em pacotes de software existentes. Portanto, o servidor Web do Apache e a extensão WebDAV sempre são executados juntamente com o subversion.

47.1.4 mailsync

Diferentemente das ferramentas de sincronização abordadas nas seções anteriores, o mailsync sincroniza somente e-mails entre caixas de correio. O procedimento pode ser aplicado em arquivos de caixas de correio locais, bem como em caixas de correio de um servidor IMAP.

Com base no ID da mensagem contido no cabeçalho do e-mail, as mensagens específicas são sincronizadas ou apagadas. A sincronização é possível entre caixas de correio específicas e entre hierarquias de caixas de correio.

47.1.5 rsync

Quando o controle de versão não é necessário, mas grandes estruturas de diretório precisam ser sincronizadas em conexões de rede lentas, a ferramenta rsync oferece mecanismos avançados para a transmissão apenas de mudanças entre arquivos. Isso não diz respeito somente a arquivos de texto, mas também a arquivos binários. Para detectar as diferenças entre os arquivos, o rsync os subdivide em blocos e realiza checksums neles.

O esforço dedicado à detecção das mudanças tem um preço. Os sistemas a serem sincronizados devem ser dimensionados generosamente para uso do rsync. A RAM é especialmente importante.

47.2 Determinando fatores para selecionar um programa.

47.2.1 Cliente-servidor versus ponto a ponto

Dois modelos diferentes são comumente usados para distribuir dados. No primeiro modelo, todos os clientes sincronizam seus arquivos com um servidor central. O servidor deve ser acessível a todos os clientes pelo menos ocasionalmente. Esse modelo é usado pelo subversion, pelo CVS e pelo WebDAV.

A outra possibilidade é deixar todos os hosts ligados em rede sincronizarem seus dados entre os pontos uns dos outros. Esse é o conceito seguido pelo unison. O rsync, na realidade, funciona no modo de cliente, mas qualquer cliente também pode atuar como um servidor.

47.2.2 Portabilidade

O subversion, o CVS e o unison também estão disponíveis para muitos outros sistemas operacionais, incluindo vários sistemas Unix e Windows.

47.2.3 Interativo versus automático

No subversion, no CVS, no WebDAV e no Unison, a sincronização de dados começa manualmente pelo usuário. Isso permite um controle fino dos dados a serem sincronizados e um fácil gerenciamento de conflitos. No entanto, se os intervalos de sincronização forem muito longos, será mais provável que ocorram conflitos.

47.2.4 Conflitos: incidência e solução

Conflitos só ocorrem raramente no subversion ou no CVS, mesmo quando muitas pessoas trabalham em um grande projeto de programa. Isso ocorre porque os documentos são fundidos na base de linhas individuais. Quando ocorre um conflito, somente um cliente é afetado. Normalmente, os conflitos no subversion ou no CVS podem ser facilmente resolvidos.

O Unison reporta conflitos, permitindo que os arquivos afetados sejam excluídos da sincronização. Entretanto, as mudanças não podem ser fundidas tão facilmente no subversion ou no CVS.

Em oposição ao subversion ou ao CVS, onde é possível aceitar parcialmente as mudanças em caso de conflito, o WebDAV só realiza o registro da entrada quando toda a modificação é considerada bem-sucedida.

Não há gerenciamento de conflitos no rsync. O usuário é responsável por não sobregravar acidentalmente arquivos e resolver manualmente todos os possíveis conflitos. Para obter segurança, é possível empregar adicionalmente um sistema de controle de versão como o RCS.

47.2.5 Selecionando e adicionando arquivos

Em sua configuração padrão, o Unison sincroniza toda uma árvore de diretórios. Novos arquivos que aparecem na árvore são incluídos automaticamente na sincronização.

No subversion ou no CVS, novos diretórios e arquivos devem ser adicionados explicitamente por meio do comando `svn add` ou o `cvs add`, respectivamente. Esse procedimento resulta em um maior controle do usuário sobre os arquivos a serem sincronizados. Por outro lado, novos arquivos são sempre ignorados, especialmente quando os pontos de interrogação na saída de `svn update` e `svn status` ou `cvs update` são ignorados devido ao grande número de arquivos.

47.2.6 Histórico

Um recurso adicional do subversion ou do CVS é a possibilidade de reconstrução de versões antigas de arquivos. Um breve comentário de edição pode ser inserido em cada mudança, e o desenvolvimento dos arquivos pode ser facilmente rastreado posteriormente

com base no conteúdo dos comentários. Essa é uma ajuda valiosa para textos de teses e de programas.

47.2.7 Volume de dados e requisitos do disco rígido

Os discos rígidos de todos os hosts envolvidos devem ter espaço em disco suficiente para todos os dados distribuídos. O subversion e o CVS requerem espaço adicional para o banco de dados repositório no servidor. O histórico do arquivo também é armazenado no servidor, requerendo ainda mais espaço. Quando arquivos em formato de texto são mudados, somente as linhas modificadas são gravadas. Arquivos binários requerem espaço em disco adicional relativo ao tamanho do arquivo sempre que ele for mudado.

47.2.8 Interface gráfica do usuário

O Unison oferece uma interface gráfica do usuário que exibe os procedimentos de sincronização a serem realizados. Aceite a proposta ou exclua arquivos específicos da sincronização. No modo de texto, confirme de forma interativa os procedimentos específicos.

Usuários experientes normalmente executam o subversion ou o CVS a partir da linha de comando. Entretanto, as interfaces gráficas do usuário estão disponíveis para Linux, como a cervisia, e para outros sistemas operacionais, como a wincvs. Muitas ferramentas de desenvolvimento, como a kdevelop, e editores de texto, como o emacs, fornecem suporte para o CVS ou o subversion. É sempre mais fácil realizar a resolução de conflitos com esses front ends.

47.2.9 Facilidade de uso

O Unison e o rsync são mais fáceis de usar e também mais adequados a usuários inexperientes. De certa forma, é mais difícil operar o CVS e o subversion. Os usuários devem entender a interação entre o repositório e os dados locais. As mudanças dos dados devem ser primeiro fundidas localmente no repositório. Esse procedimento é executado com o comando `cvs update` ou `svn update`. Em seguida, os dados devem ser enviados de volta ao repositório com o comando `cvs commit` ou

`svn commit`. Depois que esse procedimento for compreendido, os usuários inexperientes também serão capazes de usar o CVS e o subversion com facilidade.

47.2.10 Segurança contra ataques

Durante a transmissão, o ideal é proteger os dados contra interceptação e manipulação. O Unison, o CVS, o rsync e o subversion podem ser facilmente usados via ssh (secure shell - shell seguro), fornecendo segurança contra ataques deste tipo. A execução do CVS ou do Unison via rsh (remote shell - shell remoto) deve ser evitada. O acesso ao CVS com o mecanismo *pserver* em redes desprotegidas também não é recomendável. O subversion já fornece as medidas de segurança necessárias ao ser executado com o Apache.

47.2.11 Proteção contra perda de dados

O CVS tem sido usado por desenvolvedores por um longo tempo para gerenciar projetos de programas e é extremamente estável. Como o histórico do desenvolvimento é gravado, o CVS fornece proteção até mesmo contra certos erros do usuário, como uma exclusão não intencional de um arquivo. Apesar de o subversion não ser tão comum quanto o CVS, ele já está sendo empregado em ambientes de produção, por exemplo pelo projeto do próprio subversion.

O Unison ainda é relativamente novo, mas ostenta um alto nível de estabilidade. Entretanto, ele é mais sensível a erros do usuário. Depois que a sincronização da exclusão de um arquivo é confirmada, não há como restaurar o arquivo.

Tabela 47.1 *Recursos das ferramentas de sincronização de arquivos: -- = muito ruim, - = ruim ou não disponível, o = médio, + = bom, ++ = excelente, x = disponível*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Cliente/Servidor	igual	C-S/C-S	C-S	igual
Portabilidade	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interatividade	x	x/x	x	-

	unison	CVS/subv.	rsync	mailsync
Velocidade	-	o/+	+	+
Conflitos	o	++/++	o	+
Sel. de arquivos	Dir.	Sel/arq., dir.	Dir.	Caixa de Correio
Histórico	-	x/x	-	-
Espaço em disco rígido	o	--	o	+
Interface gráfica do usuário	+	o/o	-	-
Dificuldade	+	o/o	+	o
Ataques	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Perda de dados	+	++/++	+	+

47.3 Introdução ao Unison

O Unison é uma excelente solução para sincronizar e transferir árvores inteiras de diretórios. A sincronização é executada nas duas direções e pode ser controlada por meio de um front end gráfico intuitivo. Também é possível usar uma versão de console. A sincronização pode ser automatizada, de forma que a interação com o usuário não seja necessária, mas é preciso ter experiência.

47.3.1 Requisitos

O Unison deve ser instalado no cliente e no servidor. Nesse contexto, o termo *servidor* se refere a um segundo host, o host remoto (diferente do CVS, explicado na Seção 47.1.2, “CVS” (p 760)).

Na seção a seguir, o Unison será usado com o ssh. Nesse caso, um cliente SSH deve ser instalado no cliente e um servidor SSH deve ser instalado no servidor.

47.3.2 Usando o Unison

A abordagem usada pelo Unison é a associação de dois diretórios (*roots*). Essa associação é simbólica; não se trata de uma conexão online. Neste exemplo, o layout do diretório é o seguinte:

Cliente:	`/home/tux/dir1`
Servidor:	`/home/geeko/dir2`

Você deseja sincronizar esses dois diretórios. O usuário é conhecido como tux no cliente e como `geeko` no servidor. A primeira coisa a fazer é testar se a comunicação entre cliente e servidor funciona:

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Os problemas encontrados com mais freqüência são:

- As versões do Unison usadas no cliente e no servidor não são compatíveis.
- O servidor não permite conexões com SSH.
- Nenhum dos dois caminhos especificados existe.

Se tudo funcionar, omita a opção `-testserver`. Durante a primeira sincronização, o Unison ainda não conhece a relação entre os dois diretórios e envia sugestões para a direção da transferência dos arquivos e diretórios específicos. As setas da coluna *Ação* indicam a direção da transferência. Um ponto de interrogação significa que o Unison não é capaz de fazer uma sugestão com relação à direção da transferência, pois as duas versões foram mudadas ou são novas.

As teclas de seta podem ser usadas para definir a direção da transferência de entradas específicas. Se as direções de transferência estiverem corretas para todas as entradas exibidas, simplesmente clique em *Ir*.

As características do Unison (por exemplo, se ele executa a sincronização automaticamente em casos de limpeza) podem ser controladas por meio de parâmetros

de linha de comando especificados quando o programa é iniciado. Veja a lista completa de todos os parâmetros com `unison --help`.

Exemplo 47.1 *O arquivo ~/.unison/example.prefs*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Para cada par é mantido um registro de sincronização no diretório do usuário `~/.unison`. Definições de configuração, como `~/.unison/example.prefs`, também podem ser armazenadas neste diretório. Para iniciar a sincronização, especifique esse arquivo como parâmetro da linha de comando, como em `unison example.prefs`.

47.3.3 Para obter mais informações

A documentação oficial do Unison é extremamente útil. Por essa razão, esta seção simplesmente fornece uma breve introdução. O manual completo está disponível em `http://www.cis.upenn.edu/~bcpierce/unison/` e no `unison` do pacote SUSE.

47.4 Introdução ao CVS

O CVS é adequado para fins de sincronização, caso arquivos específicos sejam editados com freqüência e sejam armazenados em um formato de arquivo, como texto ASCII, ou como texto de origem de programa. O uso do CVS para sincronizar dados em outros formatos, como arquivos JPEG, é possível, mas lida com grandes quantidades de dados, pois todas as variantes de um arquivo são armazenadas permanentemente no servidor CVS. Nesses casos, não é possível usar a maioria dos recursos do CVS. O uso do CVS para sincronizar arquivos só será possível se todas as estações de trabalho puderem acessar o mesmo servidor.

47.4.1 Configurando um servidor CVS

O *servidor* é o host em que todos os arquivos válidos se localizam, incluindo as versões mais recentes de todos os arquivos. Qualquer estação de trabalho estacionária pode ser

usada como um servidor. Se possível, os dados do repositório do CVS devem ser incluídos em backups regulares.

Durante a configuração de um servidor CVS, é uma boa idéia conceder aos usuários o acesso ao servidor via SSH. Se o usuário for conhecido pelo servidor como `tux` e o software do CVS estiver instalado tanto no servidor quanto no cliente, as variáveis de ambiente a seguir deverão ser definidas no lado do cliente:

```
CVS_RSH=ssh CVS_ROOT=tux@server:/serverdir
```

O comando `cvs init` pode ser usado para inicializar o servidor CVS no lado do cliente. Esse procedimento deve ser executado apenas uma vez.

Finalmente, é necessário designar um nome à sincronização. Selecione ou crie um diretório no cliente exclusivamente para conter arquivos a serem gerenciados com o CVS (o diretório também pode ficar vazio). O nome do diretório também será o nome da sincronização. Neste exemplo, o diretório é chamado de `synchome`. Vá para esse diretório e digite o comando a seguir para definir o nome de sincronização como `synchome`:

```
cvs import synchome tux wilber
```

Vários comandos do CVS requerem um comentário. Para essa finalidade, o CVS inicia um editor (o editor definido na variável do ambiente `$EDITOR` ou vi, se nenhum editor tiver sido definido). A chamada do editor pode ser evitada se você inserir o comentário antes na linha de comando, como no exemplo a seguir:

```
cvs import –m 'this is a test' synchome tux wilber
```

47.4.2 Usando o CVS

O repositório de sincronização agora pode ter a saída registrada de todos os hosts com `cvs co synchome`. Esse procedimento cria um novo subdiretório `synchome` no cliente. Para enviar suas mudanças para o servidor, vá para o diretório `synchome` (ou um de seus subdiretórios) e digite `cvs commit`.

Por padrão, todos os arquivos (incluindo subdiretórios) são enviados para o servidor. Para enviar somente determinados arquivos ou diretórios, especifique-os em `cvs commit file1 directory1`. É necessário adicionar novos arquivos e diretórios ao repositório com um comando como `cvs add file1 directory1`,

antes de eles serem enviados para o servidor. Conseqüentemente, envie arquivos e diretórios adicionados recentemente com `cvs commit file1 directory1`.

Se você for para outra estação de trabalho, registre a saída do repositório de sincronização, caso isso não tenha sido feito em uma sessão anterior na mesma estação de trabalho (veja acima).

Inicie a sincronização com o servidor com `cvs update`. Atualize arquivos ou diretórios específicos como em `cvs update file1 directory1`. Para ver a diferença entre os arquivos atuais e versões armazenadas no servidor, use o comando `cvs diff` ou `cvs diff file1 directory1`. Use `cvs -nq update` para ver quais arquivos seriam afetados por uma atualização.

Estes são alguns símbolos de status exibidos durante uma atualização:

U
: A versão local foi atualizada. Isso afeta todos os arquivos fornecidos pelo servidor e ausentes no sistema local.

S
: A versão local foi modificada. Se havia mudanças no servidor, foi possível fundir as diferenças na cópia local.

P
: A versão local foi corrigida com a versão do servidor.

C
: O arquivo local está em conflito com a versão atual do repositório.

?
: Este arquivo não existe no CVS.

O status `M` indica um arquivo modificado localmente. Envie a cópia local para o servidor ou remova o arquivo local e execute a atualização novamente. Nesse caso, o arquivo ausente será recuperado do servidor. Se você enviar um arquivo modificado localmente e ele tiver sido mudado na mesma linha de comando e enviado, poderá haver um conflito, indicado por `C`.

Nesse caso, observe as marcas de conflito (»> e «<) no arquivo e decida entre as duas versões. Como essa tarefa pode ser desagradável, você pode abandonar as mudanças, apagar o arquivo local e digitar `cvs up` para recuperar a versão atual do servidor.

47.4.3 Para obter mais informações

Esta seção simplesmente oferece uma breve introdução sobre as várias possibilidades do CVS. Uma documentação mais abrangente está disponível no seguinte URL:

```
http://www.cvshome.org/
http://www.gnu.org/manual/
```

47.5 Introdução ao Subversion

O Subversion é um sistema de controle de versão de código-fonte aberto gratuito e amplamente considerado como sucessor do CVS, o que quer dizer que os recursos apresentados pelo CVS normalmente também estão presentes no subversion. Ele é especialmente recomendável quando as vantagens do CVS são almejadas sem que seja necessário tolerar as desvantagens. Muitos desses recursos já foram apresentados brevemente na Seção 47.1.3, “subversion” (p 761).

47.5.1 Instalando um servidor Subversion

A instalação de um banco de dados repositório em um servidor é um procedimento relativamente simples. O Subversion fornece uma ferramenta de administração dedicada para essa finalidade. Digite o comando a seguir para criar um novo repositório:

```
svnadmin create /path/to/repository
```

Outras opções podem ser relacionadas com `svnadmin help`. Em oposição ao CVS, o subversion não é baseado no RCS, mas sim no Banco de dados Berkeley. Não instale um repositório em sistemas de arquivos remotos, como NFS, AFS ou Windows SMB. O banco de dados requer mecanismos de bloqueio POSIX, não suportados por esses sistemas de arquivos.

O comando `svnlook` fornece informações sobre um repositório existente.

```
svnlook info /path/to/repository
```

É necessário configurar um servidor para permitir que usuários diferentes acessem o repositório. Use o servidor Web do Apache com o WebDAV para fazer isso, ou use o svnserve, , servidor do pacote do subversion. Quando o svnserve estiver em execução, o repositório poderá ser acessado com um URL com `svn://` ou `svn+ssh://`.

Usuários que podem se autenticar chamando `svn` podem ser definidos em `/etc/svnserve.conf`.

A decisão sobre o uso do Apache ou do svnserce depende de vários fatores. É recomendável pesquisar o manual do subversion. Mais informações sobre o assunto podem ser encontradas na Seção 47.5.3, “Para obter mais informações” (p 774).

47.5.2 Utilização e operação

Use o comando `svn` (similar ao `cvs`) para acessar um repositório do subversion. O conteúdo fornecido por um servidor configurado corretamente correspondente a determinado repositório pode ser acessado por qualquer cliente com um dos seguintes comandos:

```
svn list http://svn.example.com/path/to/project
```

ou

```
svn list svn://svn.example.com/path/to/project
```

Grave um projeto existente no diretório atual (registre a saída) com o comando `svn checkout`:

```
svn checkout http://svn.example.com/path/to/project nameofproject
```

O registro da saída cria um novo subdiretório `nameofproject` no cliente. Operações (adição, cópia, renomeação, exclusão) podem ser executadas em:

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

Esses comandos também podem ser usados em diretórios. O subversion pode registrar adicionalmente propriedades de um arquivo ou diretório.

```
svn propset license GPL foo.txt
```

O exemplo anterior define o valor `GPL` para a propriedade `license`. Exiba propriedades com `svn proplist`:

```
svn proplist --verbose foo.txt
   Properties on 'foo.txt':
   license : GPL
```

Grave as mudanças no servidor com `svn commit`. Outro usuário pode incorporar suas mudanças em seu diretório de trabalho sincronizando com o servidor e usando `svn update`.

Diferentemente do CVS, o status de um diretório em operação no subversion pode ser exibido *sem* o acesso ao repositório com `svn status`. Mudanças locais são exibidas em cinco colunas, sendo a primeira a mais importante:

''
: Nenhuma mudança.

'A'
: O objeto é marcado para adição.

'D'
: O objeto é marcado para exclusão.

'M'
: O objeto foi modificado.

'C'
: O objeto está em conflito.

'I'
: O objeto foi ignorado.

'?'
: O objeto não está sendo mantido por controle de versão.

'!'
: O objeto é reportado como ausente. Este flag é exibido quando o objeto é apagado ou movido sem o comando `svn`.

'~'
: O objeto estava sendo mantido como um arquivo, mas foi substituído por um diretório, ou ocorreu o oposto.

A segunda coluna mostra o status das propriedades. O significado de todas as outras colunas pode ser lido no manual do subversion.

Use o comando `svn help` para obter a descrição de um parâmetro de um comando:

```
svn help
proplist proplist (plist, pl): List all properties on files, dirs, or
revisions.
usage: 1. proplist [PATH...]
2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

47.5.3 Para obter mais informações

O primeiro ponto de referência é a home page do projeto subversion, em http://subversion.tigris.org/. Um manual altamente recomendável pode ser encontrado no diretório file:///usr/share/doc/packages/subversion/html/book.html depois da instalação do pacote subversion-doc e também está disponível online em http://svnbook.red-bean.com/svnbook/index.html.

47.6 Introdução ao rsync

O rsync será útil quando for necessário transmitir grandes quantidades de dados regularmente, sem que haja muitas mudanças. Esse é, por exemplo, sempre o caso da criação de backups. Uma outra aplicação diz respeito a servidores para teste. Esses servidores armazenam árvores completas de diretório de servidores Web regularmente espelhadas em um servidor Web em um DMZ.

47.6.1 Configuração e operação

O rsync pode ser operado em dois modos diferentes. Ele pode ser usado para arquivar ou copiar dados. Para isso, somente um shell remoto, como o ssh, é necessário no sistema de destino. Entretanto, o rsync também pode ser usado como um daemon para fornecer diretórios à rede.

O modo de operação básica do rsync não requer qualquer configuração especial. O rsync permite diretamente o espelhamento de diretórios inteiros em outro sistema. Como exemplo, o comando a seguir cria um backup do diretório pessoal do tux em um servidor de backup chamado de sun:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

O comando a seguir é usado para reproduzir o diretório de volta:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Até esse ponto, o gerenciamento não é muito diferente do de uma ferramenta de cópia comum, como o scp.

O rsync deve ser operado no modo "rsync" para que todos os recursos fiquem totalmente disponíveis. Isso é feito ao se iniciar o daemon rsyncd em mais de um sistema. Configure-o no arquivo `/etc/rsyncd.conf`. Por exemplo, para tornar o diretório `/srv/ftp` disponível com o rsync, use a seguinte configuração:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer
logging = true
log format = %h %o %f %l %b log file = /var/log/rsyncd.log

[FTP]
path = /srv/ftp
comment = An Example
```

Em seguida, inicie o rsyncd com `rcrsyncd start`. O rsyncd também pode ser iniciado automaticamente durante o processo de inicialização. Configure esse recurso ativando esse serviço no editor de níveis de execução fornecido pelo YaST ou digitando manualmente o comando `insserv rsyncd`. O rsyncd também pode ser iniciado com xinetd. Entretanto, isso só é recomendável para servidores que raramente usam o rsyncd.

O exemplo também cria um arquivo de registro listando todas as conexões. Esse arquivo é armazenado em `/var/log/rsyncd.log`.

Então será possível testar a transferência de um sistema cliente. Faça isso com o seguinte comando:

```
rsync -avz sun::FTP
```

Esse comando lista todos os arquivos presentes no diretório `/srv/ftp` do servidor. Essa solicitação também é registrada no arquivo de registro `/var/log/rsyncd .log`. Para iniciar uma transferência real, forneça um diretório de destino. Use `.` para o diretório atual. Por exemplo:

```
rsync -avz sun::FTP .
```

Por padrão, nenhum arquivo será apagado durante a sincronização com o rsync. Se esse procedimento for forçado, a opção adicional `--delete` deverá ser expressa. Para garantir que nenhum arquivo novo seja apagado, use a opção `--update` como alternativa. Qualquer conflito ocorrido deve ser resolvido manualmente.

47.6.2 Para obter mais informações

Informações importantes sobre o rsync são fornecidas nas páginas de manual `man rsync` e `man rsyncd.conf`. Uma referência técnica sobre os princípios de operação do rsync pode ser encontrada em `/usr/share/doc/packages/rsync/tech_report.ps`. Encontre as notícias mais recentes sobre o rsync no site do projeto, em http://rsync.samba.org/.

47.7 Introdução ao mailsync

O mailsync é principalmente adequado para as três tarefas a seguir:

- Sincronização de e-mails armazenados localmente com e-mails armazenados em um servidor
- Migração de caixas de correio de um formato diferente ou de um servidor diferente
- Verificação de integridade de uma caixa de correio ou pesquisa de duplicatas

47.7.1 Configuração e uso

O mailsync faz a distinção entre a própria caixa de correio (o *armazenamento*) e a conexão entre duas caixas de correio (o *canal*). As definições de armazenamentos e canais estão em `~/.mailsync`. Os parágrafos a seguir explicam alguns exemplos de armazenamento.

Uma simples definição pode ser exibida como a seguir:

```
store saved-messages { pat Mail/saved-messages
prefix  Mail/
}
```

O `Mail/` é um subdiretório do diretório pessoal do usuário que contém pastas de e-mail, incluindo a pasta `saved-messages`. Se o mailsync for iniciado com `mailsync -m saved-messages`, ele listará um índice de todas as mensagens em `saved-messages`. Se a definição a seguir for feita

```
store localdir {
pat     Mail/*
prefix  Mail/
}
```

o comando `mailsync -m localdir` listará todas as mensagens armazenadas em `Mail/`. Em contraste, o comando `mailsync localdir` relaciona os nomes da pasta. As especificações de um armazenamento em um servidor IMAP são exibidas como a seguir:

```
store imapinbox {
server {mail.edu.harvard.com/user=gulliver}
ref    {mail.edu.harvard.com}
pat    INBOX
}
```

O exemplo acima se refere simplesmente à pasta principal do servidor IMAP. Um armazenamento das subpastas seria exibido da seguinte forma:

```
store imapdir {
server {mail.edu.harvard.com/user=gulliver}
ref {mail.edu.harvard.com}
pat INBOX.*
prefix  INBOX.
}
```

Se o servidor IMAP suportar conexões criptografadas, as especificações do servidor devem mudar para

```
server {mail.edu.harvard.com/ssl/user=gulliver}
```

ou, se o certificado do servidor não for conhecido, para

```
server {mail.edu.harvard.com/ssl/novalidate-cert/user=gulliver}
```

O prefixo será explicado posteriormente.

Agora, as pastas em `Mail/` devem ser conectadas aos subdiretórios do servidor IMAP.

```
channel folder localdir imapdir {
msinfo .mailsync.info
}
```

O mailsync usa o arquivo `msinfo` para manter o rastreamento de mensagens que já tenham sido sincronizadas.

O comando `mailsync folder` faz o seguinte:

- Expande a caixa de correio padrão em ambos os lados.
- Remove o prefixo dos nomes de pasta resultantes.
- Sincroniza as pastas em pares (ou os cria, caso não existam).

Dessa maneira, a pasta `INBOX.sent-mail` do servidor IMPA é sincronizada com a pasta local `Mail/sent-mail` (desde que as definições explicadas acima existam). A sincronização entre a pasta específica é realizada como a seguir:

- Se uma mensagem já existir em ambos os lados, nada acontecerá.
- Se a mensagem estiver ausente em um dos lados e for nova (não listada no arquivo `msinfo`), ela será transmitida aqui.
- Se a mensagem simplesmente existir em um dos lados e for antiga (já listada no arquivo `msinfo`), ela será apagada (pois a mensagem que obviamente existia do outro lado foi apagada).

Para saber com antecedência quais mensagens serão transmitidas e quais serão apagadas durante uma sincronização, inicie o mailsync com um canal *e* um armazenamento com `mailsync folder localdir`. Esse comando produz uma lista de todas as mensagens novas nos hosts locais, bem como uma lista de todas as mensagens que seriam apagadas no lado do IMAP durante uma sincronização. Da mesma forma, o comando `mailsync folder imapdir` produz uma lista de todas as mensagens novas no lado do IMAP e uma lista de todas as mensagens que devem ser apagadas do host local durante uma sincronização.

47.7.2 Problemas possíveis

No caso de perda de dados, o método mais seguro é apagar o arquivo de registro do canal relevante `msinfo`. Conseqüentemente, todas as mensagens que existam somente em um lado serão vistas como novas e, portanto, transmitidas durante a próxima sincronização.

Somente mensagens com um ID são incluídas na sincronização. Mensagens sem ID são simplesmente ignoradas, o que significa que não são transmitidas nem apagadas. Um ID de mensagem ausente normalmente é causado por programas com falhas no envio ou na gravação de uma mensagem.

Em certos servidores IMAP, a pasta principal é chamada de `INBOX` e as subpastas são chamadas de um nome selecionado ao acaso (em contraste com INBOX e INBOX.name). Portanto, não é possível especificar um padrão exclusivamente para as subpastas dos servidores IMAP.

Depois da transmissão bem-sucedida de mensagens para um servidor IMAP, os drivers da caixa de correio (c-client) usados pelo mailsync definem um flag de status especial. Por essa razão, alguns programas de e-mail, como mutt, não são capazes de reconhecer essas mensagens como novas. Desabilite a configuração desse flag de status especial com a opção `-n`.

47.7.3 Para obter mais informações

O `README` in `/usr/share/doc/packages/mailsync/`, incluído em `mailsync`, fornece informações adicionais. Nesse contexto, o RFC 2076 “Common Internet Message Headers” é de especial interesse.

48 Samba

Com o Samba, uma máquina Unix pode ser configurada como um servidor de arquivos e de impressão para máquinas em DOS, Windows e OS/2. O Samba se tornou um produto completo e bastante complexo. Além de descrever a funcionalidade básica, este capítulo apresenta os princípios da configuração do Samba e descreve os módulos YaST que podem ser usados para configurar o Samba na sua rede.

Informações detalhadas sobre o Samba estão disponíveis na documentação digital. Digite `apropos samba` na linha de comando para exibir algumas páginas do manual ou simplesmente navegue pelo diretório `/usr/share/doc/packages/samba` se o Samba estiver instalado para obter mais documentação e exemplos online. Uma configuração de exemplo comentada (`smb.conf.SuSE`) pode ser encontrada no subdiretório `exemplos`.

Alguns novos recursos importantes da versão 3 que vem com o pacote `samba` incluem:

- Suporte ao Active Directory
- Suporte aperfeiçoado ao Unicode
- Os mecanismos de autenticação interna passaram por uma revisão completa
- Suporte aperfeiçoado para o sistema de impressão do Windows 200x e XP
- Os servidores podem ser configurados como servidores membros nos domínios do Active Directory

- A adoção de um domínio do NT4, possibilitando a migração deste último para um domínio do Samba

DICA: Migração para o Samba3

Alguns pontos especiais devem ser levados em consideração ao se migrar do Samba 2.x para o Samba 3. Uma discussão desse tópico aparece na Coleção HOWTO do Samba, onde um capítulo inteiro é dedicado ao assunto. Depois de instalar o pacote `samba-doc`, encontre o HOWTO em `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

O Samba usa o protocolo SMB (bloco de mensagens do servidor), que é baseado nos serviços NetBIOS. Devido à pressão da IBM, a Microsoft lançou o protocolo para que outros fabricantes de software pudessem estabelecer conexões com uma rede de domínio Microsoft. Com o Samba, o protocolo SMB opera acima do protocolo TCP/IP, de modo que este último precisa estar instalado em todos os clientes.

O NetBIOS é uma interface de software (API) projetada para a comunicação entre máquinas. Nesse caso, é prestado um serviço de nome. Ele permite que máquinas conectadas à rede reservem nomes para si. Após a reserva, essas máquinas podem ser tratadas pelo nome. Não há um processo central para a verificação de nomes. Qualquer máquina da rede pode reservar quantos nomes quiser, contanto que os nomes não estejam em uso ainda. A interface NetBIOS passa a poder ser implementada para diferentes arquiteturas de rede. Uma implementação que funciona com relativa proximidade com o hardware da rede é chamada de NetBEUI, mas ela muitas vezes é chamada de NetBIOS. Os protocolos de rede implementados com o NetBIOS são o IPX da Novell (NetBIOS via TCP/IP) e TCP/IP.

Os nomes de NetBIOS enviados por TCP/IP não possuem nada em comum com os nomes usados em `/etc/hosts` ou com os nomes definidos pelo DNS. O NetBIOS usa sua própria convenção de nomes independente. Contudo, é recomendável usar nomes que correspondam aos nomes de hosts DNS para facilitar a administração. Esse é o padrão usado pelo Samba.

Todos os sistemas operacionais comuns, como Mac OS X, Windows e OS/2, prestam suporte ao protocolo SMB. O protocolo TCP/IP precisa estar instalado em todos os computadores. O Samba fornece um cliente para as diferentes versões do UNIX. No caso do Linux, há um módulo de kernel para SMB que permite a integração de recursos SMB no nível de sistema Linux.

Os servidores SMB oferecem espaço em hardware a seus clientes por meio de compartilhamentos. Um compartilhamento inclui um diretório e seus subdiretórios no servidor. Ele é exportado por meio de um nome e pode ser acessado pelo nome. O nome do compartilhamento pode ser definido por qualquer nome; não precisa ser o nome do diretório de exportação. Uma impressora também recebe um nome. Os clientes podem acessar a impressora pelo nome.

48.1 Configurando o servidor

Se você pretende usar o Samba como um servidor, instale `samba`. Inicie os serviços necessários ao Samba com `rcnmb start && rcsmb start` e use `rcsmb stop && rcnmb stop` para interrompê-los.

O principal arquivo de configuração do Samba é o `/etc/samba/smb.conf`. Esse arquivo pode ser dividido em duas partes lógicas. A seção `[global]` contém as configurações central e global. As seções `[share]` contêm os compartilhamentos individuais de arquivo e impressora. Com essa abordagem, detalhes relativos aos compartilhamentos podem ser definidos de forma diferenciada ou global na seção `[global]`, que aumenta a transparência estrutural do arquivo de configuração.

48.1.1 A seção global

Os seguintes parâmetros da seção `[global]` precisam de ajustes para atender aos requisitos de configuração da sua rede para que outras máquinas possam acessar seu servidor Samba via SMB em um ambiente Windows.

workgroup = TUX-NET
: Essa linha designa o servidor Samba a um grupo de trabalho. Substitua o `TUX-NET` por um grupo de trabalho apropriado do seu ambiente de rede. Seu servidor Samba aparece sob o nome DNS, a menos que esse nome tenha sido designado a alguma outra máquina na rede. Se o nome DNS não estiver disponível, defina o nome do servidor usando `netbiosname=MYNAME`. Consulte `mansmb.conf` para obter mais detalhes sobre esse parâmetro.

os level = 2
: Esse parâmetro determina se o seu servidor Samba tenta se tornar um LMB (local master browser) para seu grupo de trabalho. Escolha um valor bem reduzido para

poupar a rede do Windows existente de perturbações causadas por um servidor Samba mal configurado. Mais informações sobre esse importante tópico podem ser encontradas nos arquivos `BROWSING.txt` e `BROWSING-Config.txt`, no subdiretório `textdocs` da documentação do pacote.

Se nenhum outro servidor SMB estiver presente na rede (como o servidor Windows NT ou 2000) e você desejar que o servidor Samba mantenha uma lista de todos os sistemas presentes no ambiente local, ajuste o `os level` em um valor mais alto (por exemplo, `65`). Assim, o servidor Samba é selecionado como LMB para a rede local.

Ao mudar essa configuração, reflita bem sobre como isso pode afetar um ambiente de rede Windows existente. Primeiro, teste as mudanças em uma rede isolada ou em um horário não crítico do dia.

suporte WINS e servidor WINS
Para integrar o servidor Samba a uma rede Windows existente dotada de um servidor WINS ativo, habilite a opção `wins server` e defina seu valor para o endereço IP desse servidor WINS.

Se as suas máquinas do Windows estiverem conectadas a sub-redes separadas e ainda assim precisarem levar as restantes em consideração, será necessário configurar um servidor WINS. Para transformar um servidor Samba em um servidor WINS, defina a opção `wins support = Yes`. Verifique se somente um servidor Samba da rede possui essa configuração habilitada. As opções `wins server` e `wins support` nunca devem ficar habilitadas ao mesmo tempo no arquivo `smb.conf`.

48.1.2 Compartilhamentos

Os exemplos a seguir ilustram como uma unidade de CD-ROM e os diretórios do usuário (`homes`) são disponibilizados aos clientes SMB.

[cdrom]
Para evitar a disponibilização acidental da unidade de CD-ROM, essas linhas são desativadas com marcas de comentários (nesse caso, pontos-e-vírgulas). Remova os pontos-e-vírgulas da primeira coluna para compartilhar a unidade do CD-ROM com o Samba.

Exemplo 48.1 *Compartilhamento de CD-ROM*

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` e `comment`
A entrada `[cdrom]` é o nome do compartilhamento que pode ser visto por todos os clientes SMB na rede. Um `comment` adicional pode ser feito para enriquecer a descrição do compartilhamento.

`path = /media/cdrom`
`path` exporta o diretório `/media/cdrom`.

Por meio de uma configuração padrão bastante restritiva, esse tipo de compartilhamento somente é disponibilizado aos usuários presentes nesse sistema. Se esse compartilhamento precisar ser disponibilizado a todos, adicione uma linha `guest ok = yes` à configuração. Essa configuração concede permissões de leitura a todos na rede. Recomenda-se muita cautela no manejo desse parâmetro. Isso se aplica ainda mais intensamente ao uso desse parâmetro na seção `[global]`.

`[homes]`
O compartilhamento `[home]` possui especial importância aqui. Se o usuário possuir uma conta e senha válidas para o servidor de arquivos Linux e seu próprio diretório pessoal, pode ficar conectado a ele.

Exemplo 48.2 *Share homes*

```
[homes]
 comment = Home Directories
 valid users = %S
 browseable = No
 read only = No
 create mask = 0640
 directory mask = 0750
```

[homes]
Contanto que não haja nenhum outro compartilhamento usando o nome de compartilhamento do usuário que estabelece a conexão ao servidor SMB, um compartilhamento é gerado dinamicamente usando as diretivas de compartilhamento `[homes]`. O nome resultante do compartilhamento é o nome do usuário.

valid users = %S
: `%S` é substituído pelo nome concreto do compartilhamento logo que uma conexão tenha sido estabelecida com sucesso. Para um compartilhamento `[homes]`, sempre será usado o nome do usuário. Conseqüentemente, os direitos de acesso ao compartilhamento de um usuário ficam restritos exclusivamente a ele.

browseable = No
: Essa configuração torna o compartilhamento invisível no ambiente da rede.

read only = No
: Por padrão, o Samba proíbe o acesso de gravação aos compartilhamentos exportados por meio do parâmetro `read only = Yes`. Para tornar um compartilhamento gravável, defina o valor `read only = No`, que corresponde a `writeable = Yes`.

create mask = 0640
: Como os sistemas que não se baseiam no MS Windows NT não compreendem o conceito de permissões do UNIX, não são capazes de designar permissões ao criar um arquivo. O parâmetro `create mask` define as permissões de acesso designadas a arquivos recém-criados. Isso somente se aplica a compartilhamentos graváveis. Na verdade, essa configuração significa que o proprietário possui permissões de leitura e gravação e que os membros do grupo principal do proprietário possuem permissões de leitura. `valid users = %S` impede o acesso de leitura mesmo se o grupo possuir permissões de leitura. Para que o grupo tenha acesso de leitura ou gravação, desative a linha `valid users = %S`.

48.1.3 Níveis de segurança

O protocolo SMB é derivado do universo DOS e Windows e leva diretamente em consideração o problema da segurança. Cada acesso a compartilhamento pode ser protegido com uma senha. O SMB possui três formas de verificar as permissões:

Segurança no nível do compartilhamento (security = share):
: Uma senha é rigorosamente designada a um compartilhamento. Todos que conheçam essa senha possuem acesso ao compartilhamento.

Segurança no nível do usuário (security = user):
Essa variação introduz o conceito do usuário ao SMB. Cada usuário precisa se registrar no servidor com sua própria senha. Após o registro, o servidor pode conceder acesso a compartilhamentos exportados específicos condicionados a nomes de usuários.

Segurança no nível do servidor (security = server):
Para seus clientes, o Samba age como se estivesse operando em modo de nível de usuário. Entretanto, ele encaminha todas as consultas de senha a outro servidor de modo de nível de usuário, que se encarrega da autenticação. Essa configuração pressupõe um parâmetro adicional (`password server =`).

A distinção entre segurança no nível de compartilhamento, usuário e servidor se aplica ao servidor inteiro. Não é possível oferecer compartilhamentos individuais de uma configuração de servidor com segurança no nível de compartilhamento e outros com segurança no nível de usuário. Entretanto, é possível executar um servidor Samba separado para cada endereço IP configurado em um sistema.

Para obter mais informações sobre esse assunto, consulte a Coleção HOWTO do Samba. No caso de vários servidores em um sistema, preste atenção nas opções `interfaces` e `bind interfaces only`.

DICA

Para tarefas administrativas simples com o servidor Samba, há também o swat de programa. Ele oferece uma interface da Web simples com a qual configurar o servidor Samba de forma prática. Em um browser, abra `http://localhost:901` e efetue login como usuário `root`. Contudo, o swat também precisa ser ativado nos arquivos `/etc/xinetd.d/samba` e `/etc/services`. Para fazer isso no arquivo `/etc/xinetd.d/samba`, edite a linha `disable` de tal modo que indique `disable = no`. Mais informações sobre o swat estão disponíveis na página do manual.

48.2 Samba como servidor de login

Em redes onde se encontram predominantemente clientes Windows, muitas vezes é preferível que os usuários somente possam se registrar com uma conta e senha válidos. Isso pode ser feito com a ajuda de um servidor Samba. Em uma rede baseada no

Windows, essa tarefa fica a cargo de um servidor Windows NT configurado como um controlador de domínio primário (PDC). As entradas a serem feitas na seção `[global]` de `smb.conf` aparecem em Exemplo 48.3, “Seção global em smb.conf” (p 788).

Exemplo 48.3 *Seção global em smb.conf*

```
[global]
 workgroup = TUX-NET
 domain logons = Yes
 domain master = Yes
```

Se forem usadas senhas criptografadas para fins de verificação (essa é a configuração padrão com instalações bem mantidas do MS Windows 9x, MS Windows NT 4.0 do pacote de serviços 3, e todos os produtos posteriores) o servidor Samba precisará ser capaz de tratá-las. A entrada `encrypt passwords = yes` na seção `[global]` permite isso (com a versão 3 do Samba, esse passa a ser o padrão). Além disso, é necessário preparar contas e senhas de usuários em formato de criptografia compatível com o Windows. Para isso, use o comando `smbpasswd -a name`. Crie a conta de domínio dos computadores, exigida pelo conceito de domínio do Windows NT, com os seguintes comandos:

Exemplo 48.4 *Configurando uma conta de máquina*

```
useradd hostname\$
smbpasswd -a -m hostname
```

Com o comando `useradd`, um símbolo de cifrão é adicionado. O comando `smbpasswd` insere esse símbolo automaticamente quando o parâmetro `-m` é usado. O exemplo de configuração comentado (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) contém configurações que automatizam essa tarefa.

Exemplo 48.5 *Configuração automatizada de uma conta de máquina*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Para verificar se o Samba pode executar esse script corretamente, escolha um usuário do Samba com as permissões de administrador obrigatórias. Para isso, selecione um usuário e adicione-o ao grupo `ntadmin`. Depois disso, será possível designar a todos os usuários pertencentes a esse grupo Linux o status de `Domain Admin` com o comando:

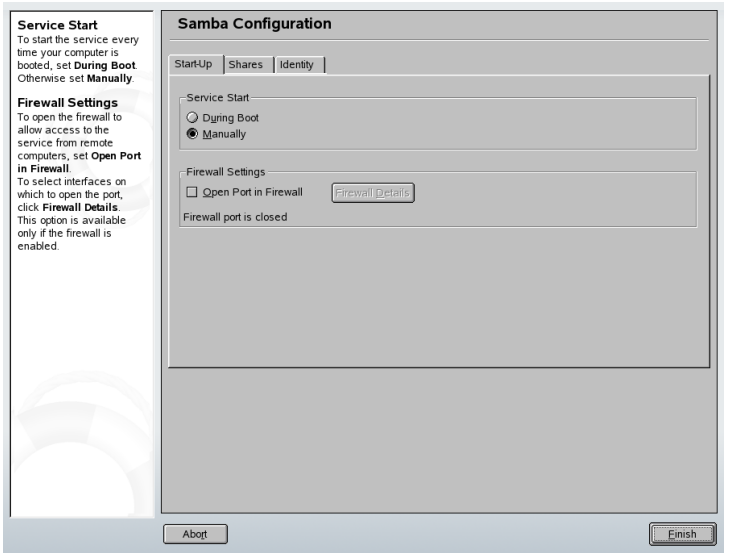
```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Mais informações sobre esse tópico aparecem no Capítulo 12 da Coleção HOWTO do Samba, contida no arquivo `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

48.3 Configurando um servidor Samba com o YaST

Para iniciar a configuração do servidor, selecione o grupo de trabalho ou domínio a ser controlado pelo novo servidor Samba. Selecione um grupo ou domínio existente em *Nome de Grupo de Trabalho ou Domínio* ou digite um novo. No passo seguinte, especifique se o servidor deve operar com PDC (controlador de domínio primário) ou como BDC (controlador de domínio de backup).

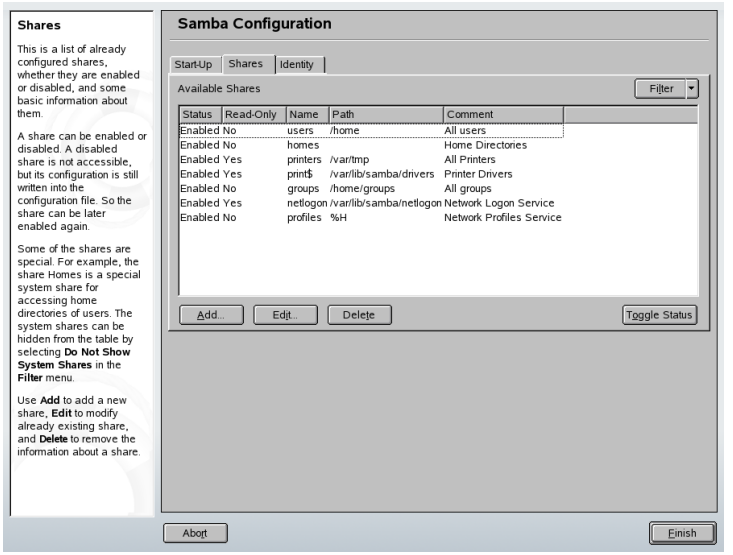
Figura 48.1 *Configuração do Samba — Inicialização*


Service Start
To start the service every time your computer is booted, set During Boot. Otherwise set Manually.
Firewall Settings
To open the firewall to allow access to the service from remote computers, set Open Port in Firewall.
To select interfaces on which to open the port, click Firewall Details. This option is available only if the firewall is enabled.
Samba Configuration
Start-Up
Shares
Identity
Service Start
During Boot
Manually
Firewall Settings
Open Port in Firewall
Firewall Details
Firewall port is closed
Abort
Finish

Ative o Samba em *Inicialização*, que aparece na Figura 48.1, “Configuração do Samba — Inicialização” (p 789). Use *Abrir Portas no Firewall* e *Detalhes do Firewall* para adaptar o firewall situado no servidor de tal modo que as portas dos serviços `netbios-ns`, `netbios-dgm`, `netbios-ssn` e `microsoft-ds` fiquem abertas

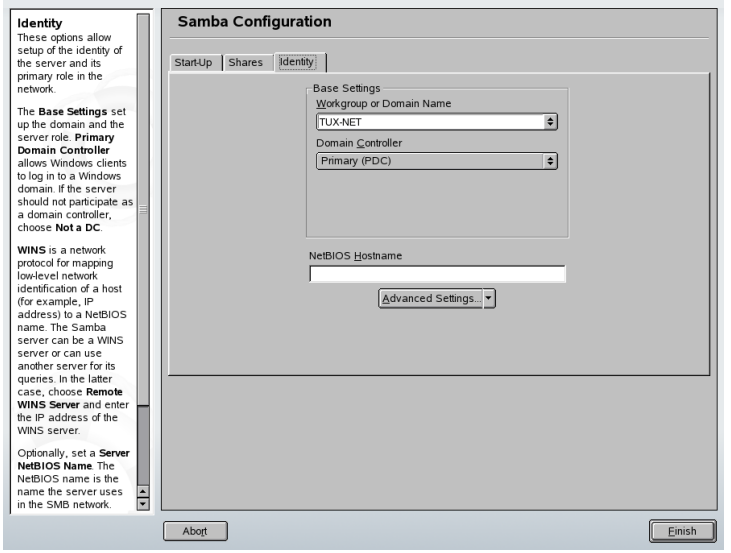
em todas as interfaces externas e internas, assegurando a suave operação do servidor Samba.

Figura 48.2 *Configuração do Samba — Compartilhamentos*


Shares
This is a list of already configured shares, whether they are enabled or disabled, and some basic information about them.
A share can be enabled or disabled. A disabled share is not accessible, but its configuration is still written into the configuration file. So the share can be later enabled again.
Some of the shares are special. For example, the share Homes is a special system share for accessing home directories of users. The system shares can be hidden from the table by selecting Do Not Show System Shares in the Filter menu.
Use Add to add a new share, Edit to modify already existing share, and Delete to remove the information about a share.
Samba Configuration
Start-Up
Shares
Identity
Available Shares
Filter
Status Read-Only Name Path Comment
Enabled No users /home All users
Enabled No homes Home Directories
Enabled Yes printers /var/tmp All Printers
Enabled Yes print$ /var/lib/samba/drivers Printer Drivers
Enabled No groups /home/groups All groups
Enabled Yes netlogon /var/lib/samba/netlogon Network Logon Service
Enabled No profiles %H Network Profiles Service
Add...
Edit...
Delete
Toggle Status
Abort
Finish

Em *Compartilhamentos* (Figura 48.2, “Configuração do Samba — Compartilhamentos” (p 790)), determine os compartilhamentos do Samba a serem ativados. Use *Alternar Status* para alternar entre *Ativo* e *Inativo*. Clique em *Adicionar* para incluir novos compartilhamentos.

Figura 48.3 *Configuração do Samba — Identidade*


Identity
These options allow setup of the identity of the server and its primary role in the network.
The Base Settings set up the domain and the server role. Primary Domain Controller allows Windows clients to log in to a Windows domain. If the server should not participate as a domain controller, choose Not a DC.
WINS is a network protocol for mapping low-level network identification of a host (for example, IP address) to a NetBIOS name. The Samba server can be a WINS server or can use another server for its queries. In the latter case, choose Remote WINS Server and enter the IP address of the WINS server.
Optionally, set a Server NetBIOS Name. The NetBIOS name is the name the server uses in the SMB network.
Samba Configuration
Start-Up
Shares
Identity
Base Settings
Workgroup or Domain Name
TUX-NET
Domain Controller
Primary (PDC)
NetBIOS Hostname
Advanced Settings...
Abort
Finish

Em *Identidade*, que aparece em Figura 48.3, “Configuração do Samba — Identidade” (p 791), determine o domínio com o qual o host deve ser associado (*Configurações de Base*) e se um nome de host alternativo deve ser usado na rede (*Nome de Host do NetBIOS*).

48.4 Configurando clientes

Os clientes somente podem acessar o servidor Samba via TCP/IP. O NetBEUI e o NetBIOS via IPX não podem ser usados com o Samba.

48.4.1 Configurando um cliente Samba com o YaST

Configure um cliente Samba para acessar recursos (arquivos ou impressoras) no servidor Samba. Digite o domínio ou grupo de trabalho na caixa de diálogo *Grupo de Trabalho Samba*. Clique em *Pesquisar* para exibir todos os grupos ou domínios disponíveis, que podem ser selecionados com o mouse. Se você ativar *Usar também informações SMB*

para a Autenticação de Linux, a autenticação do usuário será executada no servidor Samba. Após concluir todas as configurações, clique em *Concluir* para finalizar a configuração.

48.4.2 Windows 9x e ME

O Windows 9x e ME já vêm com suporte para TCP/IP. Entretanto, esse suporte não é instalado como o padrão. Para adicionar TCP/IP, vá até *Painel de Controle → Sistema* e escolha *Adicionar → Protocolos → TCP/IP da Microsoft*. Após reinicializar sua máquina com o Windows, procure o servidor Samba clicando duas vezes no ícone de área de trabalho do ambiente de rede.

DICA

Para usar uma impressora no servidor Samba, instale a unidade da impressora padrão Apple-PostScript na versão correspondente do Windows. É melhor vincular essa unidade à fila de impressão do Linux, que aceita o Postscript como um formato de entrada.

48.5 Otimização

`socket options` é uma possibilidade de otimização que acompanha a amostra de configuração que vem com a sua versão do Samba. Sua configuração padrão se refere à rede ethernet local. Para obter informações adicionais sobre `socket options`, consulte a seção pertinente das páginas do manual de `smb.conf` e a página do manual de `soquete (7)`. Outras informações são fornecidas no capítulo sobre ajuste de desempenho da Coleção HOWTO do Samba.

A configuração padrão em `/etc/samba/smb.conf` é projetada para oferecer configurações úteis com base nas configurações padrão da equipe Samba. Entretanto, uma configuração pronta para uso não é possível, principalmente no caso do nome da configuração de rede e do grupo de trabalho. A amostra de configuração comentada `examples/smb.conf.SuSE` contém informações úteis para a adaptação a requisitos locais.

DICA

A Coleção HOWTO fornecida pela equipe Samba inclui uma seção sobre a solução de problemas. Além disso, a Parte V do documento oferece um guia passo a passo para a verificação da configuração.

Índice Remissivo

Symbols

A

ACLs, 365–376
  acesso, 366, 369
  algoritmo de verificação, 375
  bits de permissão, 368
  definições, 366
  efeitos, 372
  estrutura, 367
  gerenciando, 367
  máscaras, 371
  padrão, 366, 372
  suporte, 375
ajuda
  OpenOffice.org, 162
  páginas de informações, 483
  páginas de manual, 420
  X, 552
alevt, 138
alsamixer, 117
amaroK, 120
Apache
  apxs2, 720
  arquivos binários, 717
  arquivos de configuração, 718
  arquivos de registro, 719
  cabeçalho e arquivos incluir, 719
  configurando, 720
    AccessFileName, 733
    AllowOverride, 731
    ativando, 735
    DirectoryIndex, 731
    ErrorLog, 733
    hosts virtuais, 734
    httpd.conf, 730–731
    LoadModule, 730
    LogLevel, 734
    manualmente, 728
    Módulo Apache do YaST, 721
  domínio, 712
  hosts virtuais, 737
    baseados em IP, 739
    baseados em nome, 737
    criação de álias de IP, 740
  iniciando, 735
  instalando, 713
    MPM prefork, 715
    MPM worker, 716
    módulos, 713
    YaST, 713
  módulos, 741
    extensão, 745
    módulos externos, 749
  Módulos
    Módulos de Base, 742
  parando, 735
  protocolos
    FTP, 712
    HTTP, 712
    HTTPS, 712
  segurança, 753
  solução de problemas, 754
  SSL
    configurando, 728
  terminologia, 711
aplicativos
  de escritório
    Evolution, 165
    Kontact, 179
  de multimídia
    K3b, 145
  de rede

Kontact, 179
escritório
OpenOffice.org, 155
gráficos
Digikam, 213
GIMP, 241
Kooka, 233
Linphone, 91
multimedia
KMix, 116
multimídia
amaroK, 120
audacity, 130
Grip, 127
KsCD, 125
XMMS, 124
rede
Evolution, 165
Firefox, 81
Konqueror, 75
aplicativos de e-mail
Evolution, 165–177
Kontact, 179–194
arecord, 134
arquivos
apagando, 422
arquivando, 412, 424
caminhos, 409
compactando, 412, 424
comparando, 427
convertendo dos formatos da Microsoft, 156
copiando, 421
criptografando, 348
criptografia, 110
descompactando, 413
exibindo, 410, 426
formatos
GIF, 246
JPG, 246
PAT, 246
PNG, 247
XCF, 246
localização, 481
movendo, 421
pesquisando, 425–426
pesquisando conteúdo, 426
shell, 407
sincronizando, 759–779
CVS, 760, 768–771
mailsync, 761, 776–779
rsync, 761
subversion, 761
Unison, 760, 766–768
Windows, 156
arquivos básicos, 481
arquivos de configuração, 616
.bashrc, 478, 481
.emacs, 483
.mailsync, 776
.profile, 478
.xsession, 346
/etc/fstab, 427
acpi, 281
crontab, 478
csh.cshrc, 488
dhclient.conf, 673
dhcp, 617
dhcpd.conf, 673
economia de energia, 281
exportações, 668
exports, 667
grub.conf, 463
host.conf, 620
HOSTNAME, 623
hosts, 602, 619
hotplug, 518
hwup, 520
idioma, 486, 488
ifcfg-*, 617

inittab, 441, 443–444, 485
inputrc, 485
irda, 327
kernel, 439
logrotate.conf, 480
menu.lst, 456
named.conf, 642–651
nscd.conf, 623
nsswitch.conf, 621, 701
pam_unix2.conf, 700
perfil, 488
permissões, 362
profile, 477, 481
rede, 617
redes, 620
resolv.conf, 483, 618, 642
rotas, 617
samba, 787
sem fio, 617
serviços, 787
slapd.conf, 691
smb.conf, 781, 783
smppd.conf, 625
sshd_config, 347
suseconfig, 452
sysconfig, 450–452
termcap, 485
xorg.conf, 547
Dispositivo, 551
Monitor, 552
Tela, 549
arquivos de registro, 479
boot.msg, 281
mensagens, 341, 642
Unison, 768
XFree86, 561
Assinando chaves no
KGpg, 106
audacity, 130
autenticação
PAM, 563–571

B

Bancos de dados
NSS, 622
Bash, 403–414
.bashrc, 478
.profile, 478
comandos, 404
curingas, 410
pipes, 411
profile, 477
recursos, 407
BIND, 641–651
Bluetooth, 259, 314
hciconfig, 321
hcitool, 320
opd, 323
pand, 322
rede, 318
sdptool, 321
browsers (Ver browsers da Web)
browsers da Web
Konqueror, 75–79
Browsers da Web
Firefox, 81–90
bzip2, 412

C

calendários
Evolution, 167, 174
Kontact, 182, 190
caminhos, 409
absolutos, 409
relativos, 409
trabalhando com, 409
cat, 426
CD
multissessão, 151

cd, 422
CD-Texto, 149
CDs
  copiando, 150
  criando, 145–152
    de dados, 145
    de áudio, 149
  imagens ISO, 151
  inicializando de, 454
  leitores, 125
  reproduzindo, 125–130
  ripando, 125–130
chgrp, 417, 423
chmod, 416, 423
chown, 417, 423
CJK, 486
clear, 432
coldplug, 522
comandos, 420–432
  ajuda, 404
  bzip2, 412
  cat, 426
  cd, 422
  chgrp, 417
  chmod, 416, 423
  chown, 417, 423
  clear, 432
  cp, 421
  date, 429
  df, 428
  diff, 427
  du, 428
  fontes-configuração, 553
  free, 429, 482
  getfacl, 370
  grep, 426
  grub, 455
  gzip, 412, 424
  halt, 432
  hotplug, 519
  kill, 430
  killall, 430
  less, 426
  ln, 422
  locate, 425–426
  lp, 501
  ls, 421
  man, 420
  mkdir, 422
  mount, 427
  mv, 421
  nslookup, 431
  passwd, 431
  ping, 430
  ps, 429
  reboot, 432
  rm, 422
  rmdir, 422
  scp, 343
  setfacl, 370
  sftp, 344
  slptool, 631
  smbpasswd, 788
  ssh, 343
  ssh-agent, 346
  ssh-keygen, 346
  su, 431
  tar, 412, 424
  telnet, 431
  top, 429
  udev, 525
  umount, 428
  updatedb, 425
commands
  chgrp, 423
  ldapadd, 697
  ldapdelete, 700
  ldapmodify, 699
  ldapsearch, 699
conexões sem fio

Bluetooth, 314
configurando, 450
DNS, 633
DSL, 611
GRUB, 455, 463
imprimindo, 495–498
IPv6, 600
IrDA, 326
ISDN, 608
modem a cabo, 611
modems, 605
redes, 603
manualmente, 613–624
roteamento, 617
Samba, 783–787
clientes, 791
SSH, 342
T-DSL, 613
configuration files
smpppd-c.conf, 626
consoles
alternando, 484
designando, 485
gráficos, 473
cp, 421
cpuspeed, 289
Criando chaves do
KGpg, 103
criptografando
arquivos, 348, 350
arquivos com o vi, 351
configurando com o YaST, 349
criando partições, 349–350
mídia removível, 351
partições, 348
criptografia, 103–111
Evolution, 169
Kontact, 185
cron, 478
curingas, 425
CVS, 760, 768–771
câmeras digitais, 211–231, 260
acessando, 212
conectando, 211
Digikam, 213–221
f-spot, 223
Konqueror, 213
protocolo PTP, 212

D

date, 429
desinstalando
GRUB, 471
Linux, 471
df, 428
DHCP, 669–677
configurando com o YaST, 670
designação de endereço estático, 675
dhcpd, 673–675
pacotes, 673
servidor, 673–675
diff, 427
Digikam, 213–221
digikam
edição de imagens, 222
digitalização
Kooka, 233–239
reconhecimento de caracteres, 238–239
diretórios
apagando, 422
caminhos, 409
criando, 422
estrutura, 404
mudando, 422
navegando, 409
discos
boot
criando, 472
discos de boot, 454

CDs, 454
dispositivos SCSI
configurando, 59
nomes de arquivo, 59
disquetes
inicializando de, 454
DNS, 601
BIND, 641–651
configurando, 633
domínios, 618
encaminhamento, 642
informações básicas, 633
iniciando, 642
mail exchanger, 602
NIC, 602
opções, 644
pesquisa reversa, 650
registro, 646
segurança e, 360
servidores de nomes, 618
solução de problemas, 642
top level domain, 601
zonas
arquivos, 648
DOS
compartilhando arquivos, 781
du, 428

E

e-mail
sincronizando, 761
mailsync, 776–779
sincronização, 258
editores
Emacs, 483–484
vi, 432
edição de imagens
digikam, 222
efetuando login
logrotate
configurando, 480
Emacs, 483–484
.emacs, 483
default.el, 484
encoding
ISO-8859-1, 487
endereços
IP, 588
endereços IP
classes, 589
designação dinâmica, 669
IPv6, 591
configurando, 600
mascarando, 334
privados, 591
Evolution, 165–177, 261
anexos, 169
assinaturas, 169
blocos de endereços, 172
calendário, 167, 174
contas, 167
contatos, 167, 172
criando mensagens, 169
criptografia, 169
Exchange, 165, 174, 176
filtros, 171
Groupwise, 174, 176
importando e-mails, 165
iniciando, 165
pastas, 170
PDAs e, 176
tarefas, 167
Exportando chaves
servidores de chaves
KGpg, 109
Exportando chaves públicas do
KGpg, 105
Extensão de teclado X (Ver teclado, XKB)

F

f-spot, 223
filtros de pacote (Ver firewalls)
Firefox, 81–90
  barra lateral, 83
  configurando, 86
  extensões, 86
  gerenciador de downloads, 86
  guias, 82
  imprimindo, 89
  iniciando, 81
  localizando na página, 83
  marcadores, 83
    gerenciando, 84
    migrando, 85
  navegando, 81
  pesquisando com, 83, 88
  temas, 87
firewalls, 331
  filtros de pacote, 331
  filtros de pacotes, 336
  SuSEfirewall2, 331, 336
Firewire (IEEE1394)
  discos rígidos, 260
fontes, 553
  central X11, 557
  indexadas do CID, 558
  TrueType, 553
  Xft, 554
free, 429

G

Gerenciador de Volumes Lógicos (Ver LVM)
gerenciadores de downloads
  Firefox, 86
gerenciamento de energia, 254, 277–297
  ACPI, 277, 280–287, 292
  APM, 277, 279–280, 292
  cpufrequency, 289
  cpuspeed, 289
  hibernação, 278
  monitor de bateria, 278
  nível de carga, 293
  powersave, 289
  standby, 278
  suspender, 278
  YaST, 297
GIMP, 241–249
  abrindo imagens, 245
  configurando, 242
  criando imagens, 244
  gravando imagens, 245
  imprimindo, 247
  iniciando, 242
  modelos, 244
  telas, 245
GNOME
  leitor de CD, 126
  som, 116
GNU, 403
gphoto2, 211
grep, 426
Grip, 127
GroupWise, 192
  dicas, 193
  diferenças de terminologia, 192
GRUB, 453–475
  comandos, 455–466
  curingas, 461
  desinstalando, 471
  device.map, 456, 462
  editor de menu, 461
  Erro de geometria do GRUB, 474
  grub.conf, 456, 463
  inicializando, 455
  JFS e GRUB, 474
  limitações, 455
  Master Boot Record (MBR), 453

menu de boot, 456
menu.lst, 456
múltiplos SOs e, 454
nomes de dispositivos, 458
nomes de partições, 458
senha de boot, 465
setores de boot, 454
shell do GRUB, 464
solução de problemas, 473
gráficas
placas
3D, 559–561
gráficos
3D, 559–561
3Ddiag, 561
diagnóstico, 560
drivers, 559
SaX, 560
solucionando problemas, 561
suporte para, 559
suporte à instalação para, 561
testando, 560
câmeras digitais, 211
editando, 241–249
edição (básica), 222
f-spot, 223
formatos de arquivo, 246
galerias, 237
GLIDE, 559–561
OpenGL, 559–561
drivers, 559
testando, 560
pixel, 241
vetor, 241
álbuns, 216
gunzip, 413
gzip, 412, 424

H

halt, 432
hardware
dispositivos SCSI, 59
ISDN, 608
hciconfig, 321
hcitool, 320
help
páginas de manual, 483
hotplug, 517–523
agente, 520
análise de erro, 522
arquivos de registro, 522
configuração
dispositivos, 520
interfaces, 520
dispositivos de armazenamento, 521
dispositivos de rede, 520
eventos, 519
gravador de eventos, 523
hwcfg, 522
módulos, 522
nomes de dispositivos, 518

I

I18N, 486
Importando chaves no
KGpg, 106
impressão, 491
xpp, 501
imprimindo, 495–498
aplicativos, de, 501
arquivo PPD, 496
conexão, 496
configurando com o YaST, 495
CUPS, 501
driver Ghostscript, 496
drivers, 496
filas, 496

Firefox, 89
GIMP, 247
impressoras GDI, 508
IrDA, 327
kprinter, 501
linha de comando, 501
porta, 496
página de teste, 497
rede, 510
Samba, 783
solução de problemas
rede, 510
inicializando
chaveiros USB, 454
configurando
YaST, 466–471
gerenciadores de boot, 454
GRUB, 453, 455–475
gráfico, 473
initramfs, 439
initrd, 439
múltiplos SOs, 454
setores de boot, 453–454
inicialização, 437
Iniciando o
KGpg, 103
init, 441
adicionando scripts, 446
inittab, 441
scripts, 444–448
instalando
GRUB, 455
internacionalização, 486
Internet
cinternet, 626
discagem, 625–627
DSL, 611
ISDN, 608
KInternet, 626
qinternet, 626
smpppd, 625–627
TDSL, 613
IrDA, 259, 325–328
configurando, 326
encerrando, 326
iniciando, 326
solução de problemas, 328

J

Java, 79
JavaScript, 79

K

K3b, 145–152
CDs de dados, 145
CDs de áudio, 149
configurando, 147
copiando CDs, 150
KAddressbook (Ver Kontact)
KAudioCreator, 128
KDE
KGpg, 103
shell, 403
kernels
caches, 482
limites, 542
KGpg, 103–111
confiando em chaves, 107
criptografia da área de transferência, 110
criptografia de arquivo, 110
criptografia de texto, 110
editor, 111
servidores de chaves, 107
KGpgx
servidores de chaves
importando chaves, 108
kill, 430
killall, 430

KMail (Ver Kontact)
KMix, 116
KNotes (Ver Kontact)
Konqueror, 75–79
  câmeras digitais, 213
  favoritos, 78
  guias, 76
  iniciando, 75
  Java, 79
  JavaScript, 79
  palavras-chave, 77
  perfis, 76
  salvando páginas da Web, 77
Kontact, 179–194, 261
  anexos, 184
  assinando, 185
  blocos de endereços, 187
  calendário, 182, 190
  contatos, 181, 187
  criando mensagens, 184
  criptografia, 185
  Exchange, 189, 191
  filtros, 186
  GroupWise, 189, 192
  Groupwise, 191
  identidades, 183
  importando mensagem, 179
  iniciando, 179
  listas de pendências, 181
  notas, 182
  pastas, 185
  PDAs, 192
  resumo, 180
Kooka, 233–239
  configurando, 237
  digitalizando, 235–236
  galeria, 237–238
  iniciando, 233
  reconhecimento de caracteres, 238
  visualizações, 234–235
KOrganizer (Ver Kontact)
KPilot, 195–202, 261
  /dev/pilot, 197
  backups, 201
  configurando, 196
  instalando programas com, 202
  KAddressBook, 198
  KOrganizer, 199
  sincronizando, 200
KPowersave, 257
KsCD, 125
KSysguard, 257

L

L10N, 486
laptops, 253–260
  gerenciamento de energia, 254, 277–289
  hardware, 253
  IrDA, 325–328
  PCMCIA, 253
  SCPM, 254, 265
  SLP, 256
LDAP, 685–710
  ACLs, 692
  adicionando dados, 696
  administrando grupos, 708
  administrando usuários, 708
  apagando dados, 700
  buscando dados, 699
  cliente LDAP do YaST, 700
  configuração do servidor, 691
  controle de acesso, 694
  ldapadd, 696
  ldapdelete, 700
  ldapmodify, 698
  ldapsearch, 699
  modificando dados, 698
  YaST

modelos, 702
módulos, 702
árvore de diretórios, 688
less, 410, 426
LFS, 541
Lightweight Directory Access Protocol (Ver LDAP)
Linphone, 91
Linux
compartilhando arquivos com outro SO, 781
desinstalando, 471
redes e, 585
Linux de 64 bits, 399
desenvolvimento de software, 400
especificações do kernel, 402
suporte ao tempo de execução, 399
ln, 422
localização, 486
locate, 425–426, 481
logrotate, 479
ls, 404, 421
LVM
YaST, 60

M

mascaramento
configurando com o SuSEfirewall2, 336
mascarando, 334
Master Boot Record (Ver MBR)
MBR, 453–454
memória
RAM, 482
mkdir, 408, 422
mobilidade, 253–262
câmeras digitais, 260
discos rígidos externos, 260
Firewire (IEEE1394), 260
laptops, 253
PDAs, 261
segurança de dados, 259
telefones celulares, 261
USB, 260
modems
cabo, 611
YaST, 605
monitoramento do sistema, 256
KPowersave, 257
KSysguard, 257
more, 410
motv, 135–138
buscando canais, 136
disparadores, 137
fonte de vídeo, 136
proporções, 137
áudio, 136
mount, 427
mountd, 668
MS-DOS
comandos, 413
sistemas de arquivos, 413
mtools, 413
mv, 421

N

NAT (Ver mascarando)
NetBIOS, 782
Network File System (Ver NFS)
Network Information Service (Ver NIS)
NFS, 663
clientes, 663
exportando, 666
importando, 664
montando, 664
permissões, 667
servidores, 665
nfsd, 668
NIS, 655–661

clientes, 660
escravos, 655–660
masters, 655–660
notebooks (Ver laptops)
nslookup, 431
NSS, 621
nxtvepg, 139
filtros, 140
importando banco de dados, 139
nós de dispositivo
udev, 525

O

Ogg Vorbis, 126
oggenc, 127
opd, 323
OpenLDAP (Ver LDAP)
OpenOffice.org, 155–163
ajuda, 162
assistentes, 157
Base, 161
Calc, 160
estilos, 160
formatos de documentos da Microsoft, 156
Impress, 161
módulos de aplicativos, 155
Navigator, 159
selecionando texto, 158
Writer, 157–160
OpenSSH (Ver SSH)
OS/2
compartilhando arquivos, 781

P

PAM, 563–571
pand, 322
partições
criptografando, 348
tabela de partição, 453
passwd, 431
PBX, 609
PCMCIA, 253, 263
IrDA, 325–328
PDAs, 261
Evolution, 176
Kontact, 192
KPilot, 195–202
permissões, 414–419
ACLs, 365–376
arquivos, 414
diretórios, 416
exibindo, 415
listas de controle de acesso, 419
mudando, 416, 423
permissões de arquivo, 480
sistemas de arquivos, 414
permissões de acesso (Ver permissões)
ping, 430
placas
rede, 602–603
vídeo, 552
Pluggable Authentication Modules (Ver PAM)
portas
53, 645
powersave, 289
configurando, 289
processos, 429
eliminando, 430
visão geral, 429
protocolo PTP, 212
protocolos
IPv6, 591
LDAP, 685
SLP, 629
SMB, 782
ps, 429
páginas da Web

arquivando, 77
páginas de informações, 483
páginas de manual, 420, 483

Q

qaRecord, 134

R

RAID
YaST, 67
RAID de software (Ver RAID)
reboot, 432
redes, 585
arquivos de configuração, 616–623
Bluetooth, 259, 318
configurando, 602–624
IPv6, 600
DHCP, 669
DNS, 601
endereço de broadcast, 590
endereço de rede de base, 590
host local, 591
IrDA, 259
máscaras de rede, 589
roteamento, 588–589
sem fio, 258
SLP, 629
TCP/IP, 585
WLAN, 258
YaST, 603
RFCs, 585
rm, 422
rmdir, 422
roteamento, 588, 617–618
estático, 617
máscaras de rede, 589
rotas, 617
roteando
mascarando, 334
RPM
segurança, 363
rsync, 761, 774
runlevels, 441–444
editando no YaST, 448
mudando, 443–444

S

Samba, 781–793
ajuda, 793
clientes, 782–783, 791–792
compartilhamentos, 783–784
configurando, 783–787
impressoras, 783
imprimindo, 792
iniciando, 783
instalando, 783
interrompendo, 783
login, 787
nomes, 782
otimizando, 792
permissões, 786
segurança, 786–787
servidores, 783–787
SMB, 782
swat, 787
TCP/IP e, 782
SCPM, 265
alternando perfis, 272
configurações avançadas, 272
gerenciando perfis, 271
grupos de recursos, 270
iniciando, 270
laptops, 254
scripts
boot.udev, 529
init.d, 441, 444–448, 624
boot, 445
boot.local, 446

boot.setup, 446
halt, 446
network, 624
nfsserver, 624, 667
portmap, 624, 667
rc, 444, 446
sendmail, 624
ypbind, 624
ypserv, 624
irda, 327
mkinitrd, 439
modify_resolvconf, 483, 618
SuSEconfig, 450–452
desabilitando, 452
sdptool, 321
segurança, 351–364
Apache, 753
assinaturas RPM, 363
ataques, 359–361
bugs e, 356, 359
dicas e truques, 361
DNS, 360
engenharia, 352
firewalls, 331
inicialização, 353, 355
local, 353–357
permissões, 355–356
rede, 357–361
relatando problemas, 364
Samba, 786
senhas, 354
sistema de arquivos criptografados, 259
SSH, 342–348
tcpd, 364
telnet, 342
terminais seriais, 353
vírus, 357
worms, 361
X e, 358
segurança de dados, 259
senhas
mudando, 431
Service Location Protocol (Ver SLP)
servidores de nomes (Ver DNS)
shells, 403–436
Bash, 403
caminhos, 409
comandos, 420–432
curingas, 410
pipes, 411
sincronização de dados, 258
e-mail, 258
Evolution, 261
Kontact, 261
KPilot, 261
sistema
desligamento, 432
limitação do uso de recursos, 481
localização, 486
reinicializando, 432
sistema de nomes de domínio (Ver DNS)
Sistema X Window (Ver X)
sistemas de arquivo
sysfs, 518
sistemas de arquivos, 531–543
ACLs, 365–376
criptografando, 348
cryptofs, 348
Ext2, 533–534
Ext3, 534–536
JFS, 537–538
LFS, 541
limitações, 541
Reiser4, 536–537
ReiserFS, 532–533
selecionando, 532
suportados, 539–541
termos, 531
XFS, 538–539
SLP, 256, 629

browser, 631
Konqueror, 631
registrando serviços, 629
slptool, 631
SMB (Ver Samba)
som
chips
Audigy, 119
em placa, 118
envy24, 119
Soundblaster Live, 119
compactação de dados
Grip, 127
KAudioCreator, 128
Konqueror, 129
Ogg Vorbis, 126
oggenc, 127
editando arquivos, 132
gravando
arecord, 134
audacity, 130
qaRecord, 134
leitores, 120–126
amaroK, 120
GNOME, 126
KsCD, 125
XMMS, 124
mixers, 115
alsamixer, 117
envy24control, 119
GNOME, 116
KMix, 116
SSH, 342–348
daemon, 344
mecanismos de autenticação, 346
pares de chaves, 344, 346
scp, 343
sftp, 344
ssh, 343
ssh-agent, 346–347
ssh-keygen, 346
sshd, 344
X e, 347
su, 431
subversion, 761, 771
suporte à instalação
placas gráficas 3D e, 561

T

tar, 412, 424
TCP/IP, 585
ICMP, 586
IGMP, 586
modelo em camadas, 586
pacotes, 587–588
TCP, 586
UDP, 586
teclado
Caracteres asiáticos, 486
Extensão de teclado X, 485
layout, 485
mapeamento, 485
compor, 485
multikey, 485
XKB, 485
tela
resolução, 551
telefones celulares, 261
telnet, 431
terminologia
diferenças do GroupWise, 192
top, 429
TV, 135–144
alevt, 138
EPG, 139
motv, 135–138
nxtvepg, 139
teletexto, 138
xawtv4, 141

U

udev, 525
  armazenamento em massa, 529
  chaves, 527
  curingas, 527
  regras, 526
  script de inicialização, 529
  substituição, 527
  sysfs, 528
  udevinfo, 528
ulimit, 481
  opções, 481
umount, 428
unidades
  desmontando, 428
  montando, 427
unidades flash, 260
unidades flexíveis
  inicializando de, 454
updatedb, 425
USB
  câmeras digitais, 211
  discos rígidos, 260
  unidades flash, 260
users
  /etc/passwd, 701
usuários
  /etc/passwd, 566

V

variables
  environment, 486
Voz por IP, 91
vídeo
  placas
    drivers, 552

W

webcams
  motv, 138
whois, 602
Windows
  compartilhando arquivos, 781
WLAN, 258

X

X
  ajuda, 552
  conjuntos de caracteres, 553
  drivers, 552
  fontes, 553
  fontes centrais X11, 557
  fontes indexadas do CID, 558
  fontes TrueType, 553
  otimizando, 547–553
  SaX2, 548
  segurança, 358
  sistemas de fontes, 553
  SSH e, 347
  tela virtual, 551
  xf86config, 548
  xft, 553
  Xft, 554
X.Org, 547
Xen, 573
  visão geral, 573
Xft, 554
XKB (Ver teclado, XKB)
XMMS, 124
xorg.conf
  Depth, 550
  Device, 550
  Display, 550
  Files, 548
  InputDevice, 548
  intensidade de cor, 550
  Linha modelo, 550
  modelines, 548

Modes, 549
Modos, 550
Monitor, 548, 550
ServerFlags, 548

Y

YaST
3D, 559
browser SLP, 631
carregador de boot
localização, 468
ordem do disco, 471
senha, 470
tipo, 467
cliente LDAP, 700
clientes NIS, 660
configuração de inicialização, 466
segurança, 470
sistema padrão, 469
tempo de espera, 469
DHCP, 670
DSL, 611
editor sysconfig, 450
gerenciamento de energia, 297
GRUB, 467
imprimindo, 495–498
ISDN, 608
LILO, 467
LVM, 60
modem a cabo, 611
modems, 605
placa de rede, 603
RAID, 67
runlevels, 448
Samba
clientes, 791
T-DSL, 613
YP (Ver NIS)